

On the density of rational points on rational elliptic surfaces

Julie DESJARDINS

Abstract

Let $\mathcal{E} \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ be a non-trivial rational elliptic surface over \mathbb{Q} with base $\mathbb{P}_{\mathbb{Q}}^1$ (with a section). We show the Zariski-density of the rational points of \mathcal{E} when \mathcal{E} is isotrivial with non-zero j -invariant and when \mathcal{E} is non-isotrivial with a fiber of type II^* , III^* , IV^* or I_m^* ($m \geq 0$). Moreover, we produce examples of non-trivial elliptic surfaces whose rational points might not be dense. However, given the result at our disposal, we conjecture that any non-trivial elliptic surface has a dense set of \mathbb{Q} -rational points.

Contents

1	Introduction	2
1.1	Outline of the paper	2
1.2	Acknowledgements	3
2	Rational elliptic surfaces	3
2.1	Minimal model of a rational elliptic surface	3
2.2	Del Pezzo surfaces of degree one	3
2.3	Isotrivial rational elliptic surfaces	4
3	Root number	4
3.1	Definition and motivation	4
3.2	Local root number at 2 and 3 of $y^2 = x^3 + \alpha x$ and $y^2 = x^3 + \alpha$	5
4	IRES with $j(T) \neq 0, 1728$	6
4.1	A theorem of Kollar and Mella	6
4.2	A non-isotrivial elliptic fibration	6
5	IRES with $j(T) = 1728$	6
5.1	A section of infinite order	6
5.2	A structure of conic bundle	10
5.3	Density on IRES with $j = 1728$	10
6	Root number on the fibers of IRES with $j(T) = 0$	11
6.1	Necessary and sufficient conditions for a constant root number	11
6.2	Local root number at 3	14
6.3	Local root number at 2	17
6.4	Proof of the Theorem 6.1	19
7	Root number on the fibers of IRES with $j(T) = 1728$	19
7.1	Necessary and sufficient condition for a constant root numbers	19
7.2	Local root number at 3	21
7.3	Local root number at 2	22
7.4	Proof of Theorem 7.1	26
8	Non-isotrivial rational elliptic surfaces	26
8.1	Known results	26
8.2	Rational elliptic surfaces with no place of multiplicative reduction	28
8.3	Geometric arguments	29
	References	31

1 Introduction

Let \mathcal{E} be an elliptic surface over $\mathbb{P}_{\mathbb{Q}}^1$, i.e. a projective algebraic surface \mathcal{E} defined over \mathbb{Q} endowed with a morphism $\pi : \mathcal{E} \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ such that, for all $t \in \mathbb{P}_{\mathbb{Q}}^1$ except a finite number, the fiber $\mathcal{E}_t := \pi^{-1}(t)$ is a smooth projective curve of genus 1. Moreover, we suppose that there exists a section $\sigma : \mathbb{P}_{\mathbb{Q}}^1 \rightarrow \mathcal{E}$ for π .

Such an elliptic surface \mathcal{E} can be written as the set of solutions in $\mathbb{P}^2 \times \mathbb{P}_{\mathbb{Q}}^1$ of an Weierstrass equation

$$\mathcal{E} : y^2 z = x^3 + A(T)xz^2 + B(T)z^3, \quad (1)$$

with $A(T), B(T) \in \mathbb{Z}[T]$. We call *generic fiber* of \mathcal{E} the elliptic curve over $\mathbb{Q}(T)$, denoted by \mathcal{E}_T , whose model is the equation (1).

For almost every $t \in \mathbb{P}_{\mathbb{Q}}^1$, the fiber $\mathcal{E}_t = \pi^{-1}(t)$ is an elliptic curve over \mathbb{Q} and the set $\mathcal{E}_t(\mathbb{Q})$ admits a group structure. By Mordell-Weil's theorem, this group decomposes as the sum of a finitely generated free group (isomorphic to \mathbb{Z}^r) and a finite group (the torsion points). The integer r is called the *Mordell-Weil rank* (or simply the *rank*) of E over \mathbb{Q} .

We prove the following theorem for rational elliptic surfaces (i.e. birational to \mathbb{P}^2) :

Theorem 1.1. *Let \mathcal{E} be a non-trivial isotrivial rational elliptic surface with non-zero j -invariant.*

1. *Then the set of rational points $\mathcal{E}(\mathbb{Q})$ is Zariski-dense in \mathcal{E} .*
2. *Moreover, if the j -invariant is not 1728, the surface is unirational over \mathbb{Q} .*

We are left with the surfaces with zero j -invariant. They are given by an Weierstrass equation of the form $y^2 = x^3 + g(T)$, where $g(T) \in \mathbb{Z}[T]$ is a polynomial of degree at most 6.

Theorem 6.1, gives precise conditions on the integers A and B for the surface

$$y^2 = x^3 + AT^6 + B$$

to have a constant root number of the fibers. This gives a description of which surfaces might have a non-dense set of rational points.

Theorem 1.1 does not always produce explicit points of infinite order. In Theorem 7.1, we study such a case and give the conditions under which an elliptic surface given by the following Weierstrass equation has constant root number:

$$y^2 = x^3 + C(A^2T^4 + B^2)x, \quad A, B, C \in \mathbb{Z} \text{ and } A, B \text{ coprime.}$$

These correspond to a case where the proof of Theorem 1.1 does not exhibit an explicit non-torsion section.

Given the results at our disposal, we put forward the following conjecture, a variant of a conjecture of Mazur [Maz92, Conjecture 4], where "real density" is replaced by "Zariski density". This conjecture is already implicit in the literature, particularly in [CCH05].

Conjecture 1.2. *Let $\mathcal{E} \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ be an elliptic surface over \mathbb{Q} . Then one of the two following propositions holds:*

1. *\mathcal{E} is a trivial surface, i.e. there exists a curve E_0 such that $\mathcal{E} \simeq E_0 \times \mathbb{P}_{\mathbb{Q}}^1$ over \mathbb{Q} . In this case, one has $\mathcal{E}(\mathbb{Q}) = E_0(\mathbb{Q}) \times \mathbb{P}_{\mathbb{Q}}^1(\mathbb{Q})$, and this can be dense or not dense depending on the number of points of $E_0(\mathbb{Q})$.*
2. *$\mathcal{E}(\mathbb{Q})$ is Zariski-dense in \mathcal{E} .*

We already have evidence (see [Man95, Hel03, Des16b]) that the rational points should be dense when the elliptic surface is non-isotrivial by means of the study of the root number of the fibers. The root number of an elliptic curve E is conjecturally equal to $(-1)^{\text{rk} E}$ by the parity conjecture (a weaker version of the Birch and Swinnerton-Dyer conjecture). The articles mentioned above also use two conjectures of analytic number theory, the squarefree conjecture and Chowla's conjecture, which are known only for polynomial of low degree.

In this article, we give a few results on the density of non-isotrivial rational elliptic surfaces, that are unconditional.

Theorem 8.1 gives a description of the rational elliptic surfaces on which the variation of the root number is unconditional, according to Helfgott's preprint [Hel03]. Moreover, we use geometric argument to prove Theorem 8.5 : the density of rational points on rational elliptic surfaces with a singular fiber of type II^* , III^* , IV^* or I_m^* ($m \geq 0$) .

1.1 Outline of the paper

In part 2, we give a few reminders on rational elliptic surfaces and del Pezzo surfaces. In part 3, we define the root number,

In part 4, we prove the unirationality of rational elliptic surfaces with j -invariant not equal to 0 or 1728 (the second point of Theorem 1.1). In part 5, we exhibit a section on a rational elliptic surface with j -invariant equal to 1728 and from this deduce the density of its rational points. This section is not always of infinite order, but its existence completes the proof of Theorem 1.1.

In part 6, we find conditions on the coefficients of an rational elliptic surface with zero j -invariant give by the equation $y^2 = x^3 + AT^6 + B$ (with $A, B \in \mathbb{Z}$) so that the root number of the fibers always takes the value +1. In section 7, we find conditions on the coefficients of some rational elliptic surfaces with j -invariant 1728 given by the equation $y^2 = x^3 + xC(A^2T^4 + B^2)$ (where $A, B, C \in \mathbb{Z}$) so that the root number of the fibers always takes the value +1.

We end the article in part 8 with results on non-isotrivial elliptic surfaces.

1.2 Acknowledgements

I thank my supervisor, M. Hindry, for numerous helpful conversations and suggestions and for his encouragement. I thank D. Rohrlich and J.-M. Couveignes for their careful reading of earlier versions of this work.

2 Rational elliptic surfaces

Let $\mathcal{E} \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ be an elliptic surface over \mathbb{Q} given by the Weierstrass equation

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T),$$

where $A, B \in \mathbb{Z}[T]$. The discriminant is denoted by $\Delta(T) = 4A(T)^3 + 27B(T)^2$.

Proposition 2.1. (*Criteria of rationality [Mir89]*)

An elliptic surface is rational over $\overline{\mathbb{Q}}$, if and only if

$$0 < \max\{3 \deg A, 2 \deg B\} \leq 12$$

Rational elliptic surfaces are the (non-trivial) elliptic surfaces with discriminant of lowest degree, and studying the density on them is a first step towards the resolution of Conjecture 1.2.

2.1 Minimal model of a rational elliptic surface

The following theorem due to Iskovskikh links rational elliptic surfaces to Del Pezzo surfaces.

Theorem 2.2. [*Isk79, Thm. 1*]

Let \mathcal{E} be a rational elliptic surface.

Then, it has a minimal model X/\mathbb{Q} that is :

1. *either a conic bundle of degree 1,*
2. *or a Del Pezzo surface.*

A *del Pezzo surface* X is a non-singular projective algebraic surface whose anticanonical divisor is ample. Its *degree* is the integer $d \in \{1, \dots, 9\}$ corresponding to the self-intersection number (K_X, K_X) of the canonical divisor of X .

When X is a conic bundle, the work of Kollar and Mella [KM14] guarantees that the surface is \mathbb{Q} -unirational, i.e. it is dominated by the projective plane $\mathbb{P}^2 \dashrightarrow X$. In particular, the set of rational points is dense.

Suppose that X is a del Pezzo surface of degree d . When $d \geq 3$, one knows by the work of Segre and Manin [Man74] that the existence of one rational point on X implies that the surface is \mathbb{Q} -unirational. When $d = 2$, Salgado, Testa and Várilly-Alvarado [STVA14], based on a work of Manin [Man74, Thm 29.4], showed that if X contains a rational point that does not lie on an exceptional curve nor a certain quartic, then $X(\mathbb{Q})$ is Zariski-dense. If $d = 1$, the surface X has automatically a rational point: the base point of the anticanonical system. However, the results concerning density of rational points are still partial (for instance [SvL14] and [VA11]).

2.2 Del Pezzo surfaces of degree one

If we blow up the anticanonical point on X , a del Pezzo surface of degree 1, one obtain a rational elliptic surface \mathcal{E} such that the image of the neutral section is the exceptional divisor. Thus, the rational points of X are dense if and only if the rational points of \mathcal{E} are dense.

By studying the singular points on rational elliptic surfaces, we obtain the following lemma:

Lemma 2.3. *Let \mathcal{E} be a rational elliptic surface and a minimal Weierstrass model*

$$y^2 = x^3 + A(t)x + B(t),$$

where $A, B \in \mathbb{Z}[t]$ are polynomial of degree 4 and 6 respectively. We denote by X the surface obtained from \mathcal{E} by contracting its section at infinity.

Then X is a del Pezzo surface of degree 1 if and only if the only singular fibers of \mathcal{E} have type II or I_1 .

Proof. This lemma follows directly from the fact that a del Pezzo surface is smooth. Therefore, it is obtained from an elliptic surface whose only singularities are irreducible. \square

2.3 Isotrivial rational elliptic surfaces

An isotrivial rational elliptic surface takes one of the following forms:

1. $y^2 = x^3 + aH(u, v)^2x + bH(u, v)^3$ where $a, b \in \mathbb{Q}^*$ are such that $4a^3 + 27b^2 \neq 0$;
2. $y^2 = x^3 + A(u, v)x$;
3. $y^2 = x^3 + B(u, v)$,

for polynomial $A, B, H \in \mathbb{Z}[u, v]$ such that $\deg H \leq 2$, $\deg A \leq 4$ and $\deg B \leq 6$. To avoid the case where the surface is trivial, we suppose also that H is not a square, A is not a 4th-power and B is not a 6th-power.

In each cases, the singular fibers have the following configuration:

1. Every singular fiber has type I_0^* .
2. The singular fibers have either type I_0^* , III or III^* .
3. The singular fibers have either type I_0^* , II , II^* , IV or IV^* .

The only case where an isotrivial rational elliptic surface (we will shorten this appellation in writing simply *IRES*) has a del Pezzo surface of degree 1 as a minimal model is the third one, when moreover the polynomial B is squarefree and has degree ≥ 5 .

3 Root number

3.1 Definition and motivation

The root number of an elliptic curve E is expressed as the product of the local factors

$$W(E) = \prod_{p \leq \infty} W_p(E),$$

where p runs through the finite and infinite places of \mathbb{Q} , $W_p(E) \in \{\pm 1\}$ and $W_p(E) = +1$ for all p except a finite number of them. The *local root number of E in p* , $W_p(E)$, is defined in terms of the epsilon factors of the Weil-Deligne representations of \mathbb{Q}_p (see [Del73] and [Tat77]). Rohrlich [Roh93] gives an explicit formula for the local root numbers in terms of the reduction of the elliptic curve E at a prime $p \neq 2, 3$. Halberstadt [Hal98] gives tables (completed by Rizzo [Riz03]) for the local root number at $p = 2, 3$ according to the coefficients of E . Remark moreover that we always have $W_\infty(E) = -1$.

The root number is hypothetically equal to the sign $W(E) \in \{\pm 1\}$ of the conjectural functional equation of $L(E, s)$ the L -function of E :

$$\mathcal{N}_E^{(2-s)/2} (2\pi)^{s-2} \Gamma(2-s) L(E, 2-s) = W(E) \mathcal{N}_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s).$$

When we work on elliptic curves over \mathbb{Q} , such a functional equation always exists (see Wiles' work [Wil95]) and the values of the root number and the sign of the functional equation are indeed the same.

The Birch and Swinnerton-Dyer conjecture implies that the root number is related to the rank of the elliptic curve:

Conjecture 3.1 (Parity Conjecture).

$$W(E) = (-1)^{\text{rank } E(\mathbb{Q})}.$$

As a consequence of this equality, it suffices that $W(E) = -1$ for the rank of $E(\mathbb{Q})$ not to be zero and in particular for $E(\mathbb{Q})$ to be infinite.

Let \mathcal{E} be a rational elliptic surface over $\mathbb{P}_{\mathbb{Q}}^1$. The elliptic surface can be seen as a family of elliptic curves, and admits a Weierstrass equation of the form

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T),$$

with $A(T), B(T) \in \mathbb{Z}[T]$ have respectively degree less than or equal to 4 and 6.

We denote by $\Delta(T) = 4A(T)^3 - 27B(T)^2$ the discriminant and the corresponding homogenous polynomial

$$\Delta_{\mathcal{E}}(X, Y) = Y^{12-\deg \Delta} \Delta(X/Y).$$

Let also $M_{\mathcal{E}}(X, Y)$ the product of the polynomials associated to the places of multiplicative reduction, that is to say, polynomials dividing $\Delta_{\mathcal{E}}$, but not $Y^{4-\deg A} A(X/Y)$.

We consider the sets W_+ and W_- given by

$$W_{\pm}(\mathcal{E}) = \{t \in \mathbb{Q} : \mathcal{E}_t \text{ is an elliptic curve and } W(\mathcal{E}_t) = \pm 1\}.$$

As a consequence of the parity conjecture, if $\#W_-(\mathcal{E}) = \infty$, then there exist infinitely many fibers of \mathcal{E} that are non singular elliptic curves with positive rank, and this guarantees the density of the rational points on \mathcal{E} .

When the surface is isotrivial, it can happen that one of the set W_- or W_+ is finite or empty. In [CS82], Cassels and Schinzel find a family of elliptic curves, such that $j(T) = 1728$, on which the sign of the fibers always takes the value -1 :

$$\mathcal{E}_T : y^2 = x^3 - (7 + 7T^4)^2 x.$$

Varilly-Alvarado gives more examples of elliptic surfaces with constant root number in [VA11], among them the following elliptic surface with $j = 0$, given by the Weierstrass equation

$$y^2 = x^3 + 27T^6 + 16,$$

whose fibers always have a root number of value $+1$.

3.2 Local root number at 2 and 3 of $y^2 = x^3 + \alpha x$ and $y^2 = x^3 + \alpha$

We give here some formulas for the local root number at 2 and 3 of the elliptic curves $y^2 = x^3 + \alpha x$ and $y^2 = x^3 + \alpha$ for $\alpha \in \mathbb{Q}$.

Lemma 3.2. [VA11, Lemme 4.7]

Let t be a non-zero integer and let be the elliptic curve $E_t : y^2 = x^3 + tx$. We denote by $W_2(t)$ and $W_3(t)$ its local root numbers at 2 and 3. Put t_2 and t_3 the integers such that $t = 2^{v_2(t)} t_2 = 3^{v_3(t)} t_3$. Then

$$W_2(t) = \begin{cases} -1 & \text{if } v_2(t) \equiv 1 \text{ or } 3 \pmod{4} \text{ and } t_2 \equiv 1 \text{ or } 3 \pmod{8}; \\ & \text{or if } v_2(t) \equiv 0 \pmod{4} \text{ and } t_2 \equiv 1, 5, 9, 11, 13 \pmod{16}; \\ & \text{or if } v_2(t) \equiv 2 \pmod{4} \text{ and } t_2 \equiv 1, 3, 5, 7, 11, \text{ or } 15 \pmod{16}; \\ +1 & \text{otherwise.} \end{cases}$$

$$W_3(t) = \begin{cases} -1 & \text{if } v_3(t) \equiv 2 \pmod{4}; \\ +1 & \text{otherwise.} \end{cases}$$

Lemma 3.3. [VA11, Lemme 4.1]

Let t be a non-zero integer and the elliptic curve $E_t : y^2 = x^3 + t$. We denote by $W_2(t)$ and $W_3(t)$ its local root numbers at 2 and 3. Put t_2 and t_3 the integers such that $t = 2^{v_2(t)} t_2 = 3^{v_3(t)} t_3$. Then

$$W_2(t) = \begin{cases} -1 & \text{if } v_2(t) \equiv 0 \text{ or } 2 \pmod{6}; \\ & \text{or if } v_2(t) \equiv 1, 3, 4 \text{ or } 5 \pmod{6} \text{ and } t_2 \equiv 3 \pmod{4}; \\ +1, & \text{otherwise.} \end{cases}$$

$$W_3(t) = \begin{cases} -1 & \text{if } v_3(t) \equiv 1 \text{ or } 2 \pmod{6} \text{ and } t_3 \equiv 1 \pmod{3}; \\ & \text{or if } v_3(t) \equiv 4 \text{ or } 5 \pmod{6} \text{ and } t_3 \equiv 2 \pmod{3}; \\ & \text{or if } v_3(t) \equiv 0 \pmod{6} \text{ and } t_3 \equiv 5 \text{ or } 7 \pmod{9}; \\ & \text{or if } v_3(t) \equiv 3 \pmod{6} \text{ and } t_3 \equiv 2 \text{ or } 4 \pmod{9}; \\ +1, & \text{otherwise.} \end{cases}$$

4 IRES with $j(T) \neq 0, 1728$

4.1 A theorem of Kollar and Mella

Theorem 4.1. [KM14, Thm. 1] *Let K be any field of characteristic $\neq 2$ and $a_0(t), \dots, a_3(t) \in K[t]$ polynomials of degree 2 giving a nontrivial family of elliptic curves. Then the surface*

$$S : y^2 = a_3(t)x^3 + a_2(t)x^2 + a_1(t)x + a_0(t) \subset \mathbb{A}_{x,y,t}^3$$

is unirational over K .

In a first version of the article of Kollár-Mella [KM14], Theorem 4.1 excluded the isotrivial case. The author wanted to complete this result, and obtained Theorem 4.2. However, it has been completed by Kollár and Mella themselves by the time she submitted her ph.D thesis. Their technique is different from the one in this article.

4.2 A non-isotrivial elliptic fibration

Theorem 4.2. *Let \mathcal{E} be a isotrivial rational elliptic surface given by the equation*

$$\mathcal{E} : Y^2 = X^3 + aH(T)^3X + bH(T)^2,$$

where $a, b \in \mathbb{Z} \setminus \{0\}$ and $H(T)$ is a degree ≤ 2 polynomial that is not a square. Then the surface \mathcal{E} is \mathbb{Q} -unirational. In particular, its rational points are dense for Zariski topology.

Remark 1. This result is proven by Rohrich [Roh93, Theorem 3] under the *a priori* restrictive assumption that there exists a fiber of positive rank. This assumption is removed here.

Proof. Remark that the surface \mathcal{E} is endowed with many fibrations.

$$\begin{array}{ccccc} & \mathcal{E} : H(T)Y^2 = X^3 + aX + b & & & \\ & \swarrow \varphi_1 & \downarrow \varphi_2 & \nwarrow \varphi_3 & \\ x & & y & & t \end{array}$$

The last two, φ_2 and φ_3 , are elliptic fibration (with section). Even if the fibration defined by φ_3 is isotrivial, the one defined by φ_2 is not. Indeed, if we write $H(T) = \alpha_2 T^2 + \alpha_1 T + \alpha_0$ for the appropriate coefficients α_i , the fibration φ_2 has the fiber

$$\mathcal{E}_y := \alpha_2 y^2 T^2 + \alpha_1 y^2 T = X^3 + aX + b - \alpha_0 y^2$$

which can after a change of variables (first $T' = \alpha_2 y T$ and $x = \alpha_2 X$, then $t = T' + \frac{\alpha_1 \alpha_2 y}{2}$) be written

$$\mathcal{E}_y : t^2 = x^3 - 27c_4(y)x - 54c_6(y)$$

where $c_4(y) = \alpha_2^2 a$ and $c_6(y) = (\alpha_2^3 \alpha_0 + \frac{\alpha_2^2 \alpha_1^2}{4})y^2 + \alpha_2^3 b$. By computing the j -invariant, one sees that this curve is not isotrivial, except in the case where $a = 0$ ($c_4(y)$ is zero) and $\alpha_0 = \alpha_2^3 \alpha_0 + \frac{1}{4} \alpha_1^2 \alpha_2^2$, in other words when H is the square of a linear polynomial (in that case, \mathcal{E} is trivial). These cases are excluded by our hypotheses. Hence, we can apply Theorem 4.1. This proves the unirationality of \mathcal{E} endowed with the elliptic fibration φ_2 . \square

Remark 2. Another way to prove Theorem 4.2 would have been the use the work of Colliot-Thélène [CT90]. The second theorem of this article shows that for X , a conic bundle of degree 4, the Brauer-Manin obstruction to the Hasse principle is the only obstruction. To deduce from this Theorem 4.2, one would have to check that the Brauer group of the surfaces that we consider (whose equation is $h(t)y^2 = x^3 - ax$ where $\deg h = 2$) is the Brauer-group of \mathbb{Q} .

5 IRES with $j(T) = 1728$

5.1 A section of infinite order

We study now the isotrivial rational elliptic surfaces of the form $y^2 = x^3 + xA(T)$ where $A \in \mathbb{Z}[T]$ is such that $\deg A \leq 4$. The density of rational point is easily proven in the case where $\deg A \leq 3$. For this reason, we concentrate on surfaces such that $\deg A = 4$. Let $a_4, a_3, a_2, a_1, a_0 \in \mathbb{Z}$ be the coefficients such that

$$A(T) = a_4 T^4 + a_3 T^3 + a_2 T^2 + a_1 T + a_0.$$

Remark first that we have $F(T) = a_4 \left((T^2 + g_1 T + g_0)^2 + h_1 T + h_0 \right)$, where

$$g_0 = \frac{4a_2 a_4 - a_3^2}{8a_4^2}, g_1 = \frac{a_3}{2a_4}, h_0 = \frac{2^6 a_4^3 (a_0 + x^2) - (4a_2 a_4 - a_3^2)^2}{2^6 a_4^4}$$

and

$$h_1 = \frac{2^3 a_1 a_4^2 - a_3 (4a_2 a_4 - a_3^2)}{2^3 a_4^3}.$$

We make the change of variables $T' = T - g_1/2$. We have

$$T'^4 = T^4 + \frac{g_1}{2} T^3 + \frac{6g_1^2}{4} T^2 + \frac{g_1^3}{2} T + \frac{g_1^4}{16}$$

Thus we can write

$$F(T) = a_4 (T'^4 + (\frac{-g_1^2}{2} + 2g_0) T^2 + (\frac{-g_1^3}{2} + 2g_1 g_0) T + (\frac{-g_1^4}{2^4} + g_0^2 + h_0)).$$

Replacing T^2 and T by their expressions in terms of T' , we obtain the following equation:

$$y^2 = x^3 + a_4 x (T'^4 + A_2 T'^2 + A_1 T' + A_0),$$

where

$$A_2 = (g_0 - \frac{g_1^2}{2}),$$

$$A_1 = (\frac{g_1^3}{2} + a_2 g_1)$$

and

$$A_0 = (-\frac{g_1^4}{2^4} + g_0^2 + h_0).$$

Hence, one can assume that $a_3 = 0$ (or else we do the change of variable previously explained). The surface \mathcal{E} has the following fibrations.

$$\begin{array}{ccccc} & \mathcal{E} : Y^2 = X^3 + A(T)X & & & \\ & \swarrow \varphi_1 & \downarrow \varphi_2 & \nwarrow \varphi_3 & \\ x & & y & & t \end{array}$$

The initial fibration is φ_3 . The fiber of the fibration $\varphi_1 : (x, y, t) \mapsto x$ are genus 1 curves (a priori without section). The equation of the fibre at x can be written as:

$$C_x : y^2 = a_4 x t^4 + a_2 x t^2 + a_1 x t + (a_0 x + x^3).$$

It is a genus 1 with two points at infinity, denoted by ∞_+ and ∞_- , which are rational if and only if $x \in a_4 \mathbb{Q}^{*2}$.

Proposition 5.1. *Let $P_x = cl((\infty_+) - (\infty_-)) \in C_x(\mathbb{Q})$ for $x \in a_4 \mathbb{Q}^{*2}$.*

Then

- if $a_1 = 0$, the point P_x has order 2,
- if $a_1 \neq 0$, P_x has infinite order (except for a finite number of them).

Proof. Explicitly, putting $u = \frac{1}{t}$ and $v = \frac{y}{t^2}$, one has in coordinate (u, v) :

$$\infty_+ = (0, b), \text{ and } \infty_- = (0, -b).$$

Suppose that $b^2 = a_4 x$ for a certain rational number b . We write

$$C_x : y^2 = b^2 t^4 + a_2 x t^2 + a_1 x t + a_0 x + x^3.$$

Proceed to the change of variables $Y = \frac{y}{\sqrt{a_4 x}}$ to obtain the equation:

$$C_x : Y^2 = T^4 + \frac{a_2}{a_4} T^2 + \frac{a_1}{a_4} T + \frac{a_0 + x^2}{a_4}.$$

We can write the right side of the equation under the following form:

$$G(T)^2 + H(T),$$

where

$$G(T) = T^2 + g_0, \quad H(T) = h_1 T + h_0,$$

and where the functions g_j and the h_j depend on the coefficients a_i . Explicitely, one has

$$g_0 = \frac{a_2}{2a_4}, \quad h_0 = \frac{2^2 a_4 (a_0 + x^2) - a_2^2}{2^2 a_4^2}$$

and

$$h_1 = \frac{a_1}{a_4}.$$

The equation of the curve can be written

$$(Y + G(T))(Y - G(T)) = H(T). \quad (2)$$

Put $Y + G(T) = R$, so that

$$Y - G(T) = \frac{H(T)}{R} \quad \text{and that} \quad 2G(T) = R - \frac{H(T)}{R}.$$

Moreover put $RT = S$. By multiplying the equation (2) by R , one obtain

$$2S'^2 + 2g_0 R'^2 = R'^3 - h_1 S' - h_0 R'. \quad (3)$$

Finally, one do the change of variables $(R, S) = (2R', 2S')$ to obtain the following general Weierstrass equation for C_x .

$$C_x : S^2 + \frac{h_1}{4} S = R^3 - g_0 R^2 - \frac{h_0}{4} R. \quad (4)$$

We now look at which points of this new curve are sent the two points at infinity ∞_+ and ∞_- previously mentionned. First, we find their coordinate in R . One has

$$2R = R' = Y + G(T) = \frac{y}{b} + T^2 + g_0.$$

Put $T = \frac{1}{u}$ and $y = vT^2 = \frac{v}{u^2}$ since it will be easier to study the poles. We have

$$\begin{aligned} 2R &= \frac{v}{u^2 b} + \frac{1}{u^2} + g_0 \\ &= \frac{uv + b + g_0 u^2 b}{bu^2}. \end{aligned}$$

For ∞_+ , we have $(u, v) = (0, b)$ and for ∞_- , one has $(u, v) = (0, -b)$. Hence, one has

$$R(\infty_+) = \infty \text{ (it is a pole), and } R(\infty_-) = 0.$$

Now, find the value of their coordinate in S . Remark that

$$\begin{aligned} y^2 &= G(T)^2 + H(T) \\ \Rightarrow \left(\frac{v}{u^2 b}\right) &= G\left(\frac{1}{u}\right)^2 + H\left(\frac{1}{u}\right) \\ \Rightarrow \left(\frac{v}{u^2 b} - G\left(\frac{1}{u}\right)\right) \left(\frac{v}{u^2 b} + G\left(\frac{1}{u}\right)\right) &= H\left(\frac{1}{u}\right) \\ \Rightarrow \left(\frac{v}{u^2 b} + G\left(\frac{1}{u}\right)\right) &= \frac{H\left(\frac{1}{u}\right)u^2 b}{v - u^2 G\left(\frac{1}{u}\right)b} = \frac{ub(h_1 + h_0 u)}{v(v - b - g_0 u^2)} \end{aligned}$$

$$\begin{aligned} 2S &= S' = T(Y + G(T)) \\ &= \frac{ub(h_1 + h_0 u)}{v(v - b - g_0 u^2)} \end{aligned}$$

Thus, one has

$$S(\infty_+) = \infty \text{ and } S(\infty_-) = -\frac{h_1}{4}$$

Remark that these are the two obvious points on the curve 4. We put in a natural way the point obtain from ∞_+ as marked point of the curve C_x , that is as the identity element of the group law of the set of rational points. With this configuration one has $(0, -\frac{h_1}{4}) = [-1](0, 0)$. We deduce of this that if $h_1 = \frac{a_1}{a_4} = 0$, then the point $(0, -\frac{h_1}{4})$ has order 2.

In the case where $h_1 \neq 0$, let us find the order of $Q = (0, 0)$. Remark that its order will be the same as the one obtained from ∞_- . We use a result proven simultaneously by Lutz and Nagell which can be found [Sil94, p.240]: if E/\mathbb{Q} is an elliptic curve of Weierstrass equation $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ and that $P \in E(\mathbb{Q})$ is a torsion point different for the point at infinity, then the following properties hold:

1. $x(P), y(P) \in \mathbb{Z}$.
2. We have either $[2]P = O$ or $x([2]P) \in \mathbb{Z}$.

To use this fact, we need to consider a curve with integer coefficients (denote these coefficients by A_i). As the coefficients of C_x might not be integers, we will choose a certain integer α for which the twist of the curve has integer coefficients. Let u and v be the coprime integers such that $x = \frac{u}{v}$. If we put $\alpha = 2 \cdot a_4 v$, the coefficients of the curve are integers

$$C'_x : S^2 + \alpha^3 \frac{h_1}{4} S = R^3 - \alpha^2 g_0 R^2 - \alpha^4 \frac{h_0}{4} R.$$

(In fact, it is sufficient to put $\alpha = 2a_4 w$ where w is an integer such that $v^2 \mid w$.) We now show that if $h_1 \neq 0$, the point Q is not 2-torsion for infinitely many values of x . We first find the condition for $R([2]Q)$ to be an integer. For every point $P \in C_x(\mathbb{Q})$, one has

$$R([2]P) = \left(\frac{3R(P)^2 - 2\alpha^2 g_0 R(P) - \alpha^4 \frac{h_0}{4}}{2S(P) + \frac{h_1}{4} \alpha^3} \right)^2 - 2R(P) + \alpha^2 g_0.$$

We thus have

$$R([2]Q) = \left(\frac{4\alpha^4 h_0}{4\alpha^3 h_1} \right)^2 + 4\alpha^2 g_0.$$

For this coordinate to be an integer, we need $\alpha^3 h_1$ to divide $\alpha^4 h_0$. Recall that $x = \frac{u}{v}$ where $u, v \in \mathbb{Z}$ are coprime. We have

$$\alpha^4 h_0 = A \left(\frac{u}{v} \right)^2 + B,$$

where $A = 2^4 a_4^3 v^4$ and $B = 2^4 a_4^3 a_0 u^4 - 2^2 a_4^2 a_2^2 v^4$. As for the quantity $\alpha^3 h_1$, it is an integer of value

$$\alpha^3 h_1 = 2^3 a_4^2 a_1 v^3.$$

If $\alpha^3 h_1 \mid \alpha^4 h_0$ for every $x \in \mathbb{Q}^{2*} a_4$, then $\alpha^3 h_1$ divides B (we obtain this taking for instance $x = (\alpha^3 h_1)^2 a_4$). Therefore, $\alpha^3 h_1$ divides Ax^2 for any choice of x . Choose v prime to $2a_4$. In this case, we have a contradiction since $Ax^2 = 2^3 a_4^2 v^2 (2a_4 u)$ should be divisible by $2^3 a_4^2 a_1 v^3$, but v is assumed to be prime to $2a_4$ and to u . This contradiction shows that for every $x \in \mathbb{Q}^{2*} a_4$ whose denominator is prime to $2a_4$, the point Q is of infinite order on the curve C_x .

We conclude the proof by use Silverman's specialization theorem (see [Sil83] and [Sil, Theorem 11.4, Chapter III]). A priori, the fibration

$$\begin{aligned} \varphi_2 : \mathcal{E} &\rightarrow \mathbb{P}_{\mathbb{Q}}^1 \\ (x, y, t) &\mapsto x. \end{aligned}$$

is not an elliptic surface over \mathbb{Q} . However, let us consider the application

$$\begin{aligned} \phi : \mathbb{P}_{\mathbb{Q}}^1 &\rightarrow \mathbb{P}_{\mathbb{Q}}^1 \\ z &\mapsto x = a_4 z^2. \end{aligned}$$

and the fibered product \mathcal{E}' of \mathcal{E} with respect to the fibration. By the previous argument, \mathcal{E}' admits two sections ∞_+ and ∞_- . It is thus an elliptic surface over \mathbb{Q} . Let us choose as the canonic section ∞_+ .

If there exists a linear change of variable such that $A = A_4 T'^4 + A_2 T'^2 + A_0$, then ∞_- is a torsion point on every fiber at $x = az^2$ of \mathcal{E} . Therefore, the section $\infty_+(z)$ is torsion for every $z \in \mathbb{P}_{\mathbb{Q}}^1$.

If there is no such change of variable, then the point ∞_- has infinite order for infinitely many fibers of \mathcal{E} . Therefore, Silverman's specialization theorem guarantees that $\infty_-(z)$ has infinite order on every fiber of \mathcal{E}' except for a finite number of them. \square

We directly deduce from this proposition the following theorem :

Theorem 5.2. *Let \mathcal{E} be a rational elliptic surface given by the equation*

$$\mathcal{E} : T^2 = X^3 + A(T)X,$$

where $A(T)$ is a polynomial of degree 4 with integer coefficients.

Suppose there exists no linear change of variable $T \rightarrow T' + b$ such that A is of the form

$$A(T') = A_4 T'^4 + A_2 T'^2 + A_0,$$

where $A_4, A_2, A_0 \in \mathbb{Z}$.

Then the rational points of \mathcal{E} are Zariski-dense.

Remark 3. The surfaces which are not treated by this theorem are of the form:

$$y^2 = x^3 + x(a_4 T^4 + 4ba_4 T^3 + (6b^2 a_4 + a_2)T^2 + (4b^3 + 2ba_2)T + a_4 b^4 + a_2 b^2 + a_0)$$

for a certain $b \in \mathbb{Q}$ and $a_4, a_2, a_0 \in \mathbb{Z}$ such that $\sqrt{a_2^2 - 4a_4 a_0} \notin \mathbb{Q}$.

Proof. We can assume that $a_1 = a_3 = 0$. For these surfaces, the application $(x, y, t) \mapsto x$ is a fibration in genus 1 curves, infinitely many of which (in fact every fiber at $x \in a_4 \mathbb{Q}^{*2}$ except a finite number of them) admits a structure of group and a point of infinite order. This shows the density of rational points of $\mathcal{E}(\mathbb{Q})$. \square

Suppose that the surface we consider is such that $A_1 = 0$. Proposition 5.1 shows that for almost every $x \in a_4 \mathbb{Q}^{*2}$ the elliptic curve C_x has a point of order 2, but this does not allow us to conclude on the density of rational points. Various arguments make it possible to prove the density, though.

5.2 A structure of conic bundle

Theorem 5.3. *Let \mathcal{E} be a rational elliptic surface of Weiestrass equation*

$$y^2 = x^3 + A(T^2 - \alpha)(T^2 - \beta)x,$$

where $A, \alpha, \beta \in \mathbb{Q}$. Then the rational points are Zariski-dense.

Proof. By changing variables $X = (T^2 - \alpha)x$ and $Y = (T^2 - \alpha)^2 y$, one obtain the equation

$$Y^2 = (T^2 - \alpha)X^3 + A(T^2 - \beta)(T^2 - \alpha)^4 X$$

which is isomorphic to

$$Y^2 = (T^2 - \alpha)X^3 + A(T^2 - \beta)X.$$

A reshuffle of the terms permits to obtain the following equation for \mathcal{E}

$$Y^2 - T^2(X^3 - AX) + (\alpha X^3 + XA\beta) = 0$$

which is a conic bundle. This bundle has less than 6 singular fibers. Corollary 8 of the article of Kollár and Mella [KM14] thus shows unirationality of \mathcal{E} . Therefore, the rational points are dense. \square

5.3 Density on IRES with $j = 1728$

As a conclusion for this section, we show the density of rational points on every isotrivial rational elliptic surfaces with j -invariant 1728.

Theorem 5.4. *Let \mathcal{E} be an isotrivial rational elliptic surface with $j(T) = 1728$. Then the rational points $\mathcal{E}(\mathbb{Q})$ are Zariski-dense.*

Proof. Let \mathcal{E} be an isotrivial rational elliptic surface with j -invariant $j(T) = 1728$.

Recall Theorem 2.2 due to Iskovskikh that says that a rational elliptic surface has a minimal model which is either a conic bundle of degree 1 or a del Pezzo surface.

Let X be the minimal model of \mathcal{E} . As a corollary of Lemma 2.3, X is never a del Pezzo surface of degree 1. In the case where the minimal model is a conic bundle of degree 1, [KM14] show unirationality of X , and thus the density of its rational points. Therefore, it is also the case for \mathcal{E} . In the case where the minimal model is a del Pezzo surface of degree ≥ 3 , [Man74] shows unirationality of X and \mathcal{E} .

We only have to consider the case where X is a del Pezzo surface of degree 2. In this case, we have the following sections on \mathcal{E} :

1. The section of the points at infinity $[0, y, 0, 0]$.
2. The section of Proposition 5.1 $[x, \frac{-b}{u^2}, \frac{1}{u}, 1]$ where $u = 0$, $b = \sqrt{a_4 x}$ and $x \in a_4 \mathbb{Q}^{*2}$.

3. The section $[0, 0, t, 1]$.

If the contraction two of them gives a del Pezzo surface of degree 2, then the image of the third is a rational curve. If it is an exceptional curve, we can contract it to obtain a del Pezzo of degree 3, on which the rational points are dense. If the image is not an exceptional curve, it allows all the same to find an infinity of points on X . Therefore, some of them are not on an exceptional curve nor on a distinguished quartic. We can thus use the work of Salgado, Testa and Várilly-Alvarado which shows unirationality and density of rational points on X and \mathcal{E} . \square

6 Root number on the fibers of IRES with $j(T) = 0$

Let X be a rational elliptic surface described by the Weierstrass equation

$$X : y^2 = x^3 + F(T, 1).$$

A general geometric argument to show the density of the rational points, like those presented in the previous sections, is still not known. However, we can study the variation of the root number of the fibers of X . More precisely, we will study the cardinality of the sets

$$W_{\pm}(\mathcal{E}) = \{t \in \mathbb{Q} \mid W(\mathcal{E}_t) = \pm 1\}.$$

If $\#W_{-} = \infty$, we can conclude the density of the rational points conditionally to the parity conjecture.

As illustrated by Cassels and Schinzel [CS82] and Várilly-Alvarado [VA11], there exists isotrivial elliptic surfaces with constant root number on the fibers of either values $+1$ and -1 .

6.1 Necessary and sufficient conditions for a constant root number

Notation 1. Let N be an integer, and p be a prime number. We denote N_p the integer such that $N = p^{v_p(N)} N_p$.

Theorem 6.1. *Let \mathcal{E} be an elliptic surface described by the Weierstrass equation*

$$\mathcal{E} : y^2 = x^3 + aT^6 + b,$$

where $a, b \in \mathbb{Z}$ and $C = (a, b)$.

Then, the function $t \rightarrow W(\mathcal{E}_t)$ of the root number of the fibers is constant if and only if one has $a/C = 3A^2$ and $b/C = B^2$ for integers A and B respecting an option of each of the following lists.

In particular, if we put

$$\sigma = \#\{p \text{ such that } p^2 \mid C \text{ and } p \equiv 2 \pmod{3}\},$$

the root number of the elliptic surface \mathcal{E} is equal to $W(\mathcal{E}_t) = +1$ for every non singular fiber \mathcal{E}_t ($t \in \mathbb{Q}$) if and only if

1. σ is even and the integers A, B, C in the surface equation satisfy

- (a) an option of A . and an option of 2;
- (b) an option of B . and an option of 1,

2. σ is odd and the integers A, B, C in the surface equation satisfy

- (a) an option of A . and an option of 1;
- (b) an option of B . and an option of 2.

First list :

A. One has $C_2 \equiv 3 \pmod{4}$ and one of the following cases :

- (a) $v_2(A)$ and $v_2(B) \equiv 0 \pmod{3}$ and $v_2(C) \equiv 0 \pmod{6}$
- (b) $v_2(A) \equiv 1 \pmod{3}$ et
 - i. $v_2(C) \equiv 0 \pmod{6}$
 - ii. $v_2(C) \equiv 4 \pmod{6}$
- (c) $v_2(B) \equiv 1 \pmod{3}$ and
 - i. $v_2(C) \equiv 0 \pmod{6}$
 - ii. $v_2(C) \equiv 2 \pmod{6}$
- (d) $v_2(A) \equiv 2 \pmod{3}$ and
 - i. $v_2(C) \equiv 2 \pmod{6}$

- ii. $v_2(C) \equiv 4 \pmod{6}$
- (e) $v_2(B) \equiv 2 \pmod{3}$ and
 - i. $v_2(C) \equiv 0 \pmod{6}$
 - ii. $v_2(C) \equiv 2 \pmod{6}$
- B. One has $C_2 \equiv 1 \pmod{4}$ and one of the following cases :
 - (a) $v_2(A)$ and $v_2(B) \equiv 0 \pmod{3}$ and $v_2(C) \equiv 0 \pmod{6}$
 - (b) $v_2(A) \equiv 1 \pmod{3}$ and
 - i. $v_2(C) \equiv 0 \pmod{6}$
 - ii. $v_2(C) \equiv 2 \pmod{6}$
 - (c) $v_2(B) \equiv 1 \pmod{3}$ and
 - i. $v_2(C) \equiv 0 \pmod{6}$
 - ii. $v_2(C) \equiv 4 \pmod{6}$
 - (d) $v_2(A) \equiv 2 \pmod{3}$ and
 - i. $v_2(C) \equiv 0 \pmod{6}$
 - ii. $v_2(C) \equiv 2 \pmod{6}$
 - (e) $v_2(B) \equiv 2 \pmod{3}$ and
 - i. $v_2(C) \equiv 2 \pmod{6}$
 - ii. $v_2(C) \equiv 4 \pmod{6}$

Second list :

Notation : If $v_2(A) = 0$, put $k = v_2(B) - 1$ and $A' = B_2, B' = A_2$. Otherwise, put $k = v_2(A)$ and $A' = A_2, B' = B_2$.

1. (a) $k \equiv 0 \pmod{3}$,
 - i. $v_3(C) \equiv 3 \pmod{6}$
 - A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 4 \pmod{9}$,
 - B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1 \pmod{9}$,
 - C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 7 \pmod{9}$,
 - ii. $v_3(C) \equiv 5 \pmod{6}$
 - A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
 - B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,
 - C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,
 - iii. $v_3(C) \equiv 0 \pmod{6}$
 - A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,
 - B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
 - C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,
 - iv. $v_3(C) \equiv 2 \pmod{6}$
 - A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
 - B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
 - C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
- (b) $k \equiv 1 \pmod{3}$,
 - i. $v_3(C) \equiv 0 \pmod{6}$
 - A. $C_3 \equiv 1 \pmod{9}$. $A'^2 \equiv 1, 4 \pmod{9}$ and $B'^2 \equiv 7 \pmod{9}$,
 - B. $C_3 \equiv 2 \pmod{9}$. $A'^2 \equiv 1, 4 \pmod{9}$ and $B'^2 \equiv 7 \pmod{9}$,
 - C. $C_3 \equiv 4 \pmod{9}$. $A'^2 \equiv 1, 7 \pmod{9}$ and $B'^2 \equiv 4 \pmod{9}$,
 - D. $C_3 \equiv 5 \pmod{9}$. $A'^2 \equiv 4, 7 \pmod{9}$ and $B'^2 \equiv 1 \pmod{9}$,
 - E. $C_3 \equiv 7 \pmod{9}$. $A'^2 \equiv 4, 7 \pmod{9}$ and $B'^2 \equiv 1 \pmod{9}$,
 - F. $C_3 \equiv 8 \pmod{9}$. $A'^2 \equiv 1, 7 \pmod{9}$ and $B'^2 \equiv 4 \pmod{9}$,
 - ii. $v_3(C) \equiv 1, 4 \pmod{6}$ and $C_3 \equiv 1 \pmod{3}$,
 - iii. $v_3(C) \equiv 2, 5 \pmod{6}$ and $C_3 \equiv 2 \pmod{3}$,
 - iv. $v_3(C) \equiv 3 \pmod{6}$
 - A. $C_3 \equiv 1 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,

- B. $C_3 \equiv 2 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 C. $C_3 \equiv 4 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 D. $C_3 \equiv 5 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,
 E. $C_3 \equiv 7 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
 F. $C_3 \equiv 8 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
- (c) $k \equiv 2 \pmod{3}$
- i. $v_3(C) \equiv 1 \pmod{6}$
 A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,
 B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
 C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,
- ii. $v_3(C) \equiv 3 \pmod{6}$
 A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
 B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
 C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
- iii. $v_3(C) \equiv 0 \pmod{6}$
 A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
 B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,
 C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,
- iv. $v_3(C) \equiv 4 \pmod{6}$
 A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 4 \pmod{9}$,
 B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1 \pmod{9}$,
 C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 7 \pmod{9}$,
2. (a) $k \equiv 0 \pmod{3}$,
- i. $v_3(C) \equiv 0 \pmod{6}$
 A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
 B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
 C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
- ii. $v_3(C) \equiv 2 \pmod{6}$
 A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
 B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,
 C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,
- iii. $v_3(C) \equiv 3 \pmod{6}$
 A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,
 B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
 C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,
- iv. $v_3(C) \equiv 5 \pmod{6}$
 A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 7 \pmod{9}$,
 B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 4 \pmod{9}$,
 C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 1 \pmod{9}$,
- (b) $k \equiv 1 \pmod{3}$,
- i. $v_3(C) \equiv 0 \pmod{6}$
 A. $C_3 \equiv 1 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
 B. $C_3 \equiv 2 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
 C. $C_3 \equiv 4 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,
 D. $C_3 \equiv 5 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 E. $C_3 \equiv 7 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 F. $C_3 \equiv 8 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,
- ii. $v_3(C) \equiv 1, 4 \pmod{6}$ and $C_3 \equiv 2 \pmod{3}$,
 iii. $v_3(C) \equiv 2, 5 \pmod{6}$ and $C_3 \equiv 1 \pmod{3}$,

- iv. $v_3(C) \equiv 3 \pmod{6}$
- A. $C_3 \equiv 1 \pmod{9}$. $A'^2 \equiv 4 \pmod{9}$ and $B'^2 \equiv 1, 4 \pmod{9}$,
 - B. $C_3 \equiv 2 \pmod{9}$. $A'^2 \equiv 1 \pmod{9}$ and $B'^2 \equiv 1, 4 \pmod{9}$,
 - C. $C_3 \equiv 4 \pmod{9}$. $A'^2 \equiv 1 \pmod{9}$ and $B'^2 \equiv 1, 7 \pmod{9}$,
 - D. $C_3 \equiv 5 \pmod{9}$. $A'^2 \equiv 4 \pmod{9}$ and $B'^2 \equiv 4, 7 \pmod{9}$,
 - E. $C_3 \equiv 7 \pmod{9}$. $A'^2 \equiv 7 \pmod{9}$ and $B'^2 \equiv 4, 7 \pmod{9}$,
 - F. $C_3 \equiv 8 \pmod{9}$. $A'^2 \equiv 7 \pmod{9}$ and $B'^2 \equiv 1, 7 \pmod{9}$,
- (c) $k \equiv 2 \pmod{3}$
- i. $v_3(C) \equiv 0 \pmod{6}$
 - A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
 - B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
 - C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
 - ii. $v_3(C) \equiv 1 \pmod{6}$
 - A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
 - B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
 - C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
 - iii. $v_3(C) \equiv 3 \pmod{6}$
 - A. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
 - B. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,
 - C. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,
 - iv. $v_3(C) \equiv 4 \pmod{6}$
 - A. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,
 - B. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
 - C. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,

When the surface has negative root number on every non-singular fiber, the parity conjecture states that the rank of the fibers of this elliptic surface should be always positive. For the surfaces on which the root number is $+1$, however, it is not possible to conclude anything about the density of rational points from the study of the variation of the root number.

Example 1. Let be the elliptic surface defined by the equation

$$y^2 = x^3 + 39(27T^6 + 1).$$

By Theorem 6.1, the function of the root number is constant when t runs through \mathbb{Q} . Indeed, one has $\sigma = 0$ (even), $v_2(C) = 0$, $C_2 \equiv 3 \pmod{4}$ (hence \mathcal{E} appears in list B), $v_3(C) = 1$, $v_2(A) = 1$ and $C_3 \equiv 1 \pmod{3}$ (hence \mathcal{E} appears in list 1). Therefore, one has

$$W(\mathcal{E}_t) = +1.$$

Example 2. Under the same hypotheses as in the previous exemple but with instead $C_3 \equiv 2 \pmod{3}$, the root number is -1 . This holds for the surface defined by the equation

$$y^2 = x^3 + 15(27t^6 + 1).$$

6.2 Local root number at 3

Lemma 6.2. Let \mathcal{E} be an elliptic surface given by the Weierstrass equation

$$\mathcal{E} : y^2 = x^3 + C(3A^2T^6 + B^2),$$

where $A, B, C \in \mathbb{Z}$ and $\text{pgcd}(A, B) = 1$.

When $v_2(B) = 0$, put $k = v_2(A)$, $A' = A_3$ and $B' = B_3$. If $v_2(A) = 0$, put $k = v_2(B) - l$, $A' = B_3$ and $B' = A_3$.

The function $w_3(t) = W_3(\mathcal{E}_t)(-1)^{v_3(t)}$ is constant if and only if

1. $k \equiv 0 \pmod{3}$,

(a) $v_3(C) \equiv 0 \pmod{6}$

- i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,

- ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
 - iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
 - (b) $v_3(C) \equiv 2 \pmod{6}$
 - i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
 - ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,
 - iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,
 - (c) $v_3(C) \equiv 3 \pmod{6}$
 - i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 4 \pmod{9}$,
 - ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1 \pmod{9}$,
 - iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 7 \pmod{9}$,
 - (d) $v_3(C) \equiv 5 \pmod{6}$
 - i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
 - ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,
 - iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,
 - 2. $k \equiv 1 \pmod{3}$,
 - (a) $v_3(C) \equiv 0 \pmod{6}$
 - i. $C_3 \equiv 1 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
 - ii. $C_3 \equiv 2 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
 - iii. $C_3 \equiv 4 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,
 - iv. $C_3 \equiv 5 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 - v. $C_3 \equiv 7 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 - vi. $C_3 \equiv 8 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,
 - (b) $v_3(C) \equiv 1, 2 \pmod{6}$ and $C_3 \equiv 1 \pmod{3}$,
 - (c) $v_3(C) \equiv 3 \pmod{6}$
 - i. $C_3 \equiv 1 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,
 - ii. $C_3 \equiv 2 \pmod{9}$. $B'^2 \equiv 1, 4 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 - iii. $C_3 \equiv 4 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 1 \pmod{9}$,
 - iv. $C_3 \equiv 5 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 4 \pmod{9}$,
 - v. $C_3 \equiv 7 \pmod{9}$. $B'^2 \equiv 4, 7 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
 - vi. $C_3 \equiv 8 \pmod{9}$. $B'^2 \equiv 1, 7 \pmod{9}$ and $A'^2 \equiv 7 \pmod{9}$,
 - (d) $v_3(C) \equiv 4, 5 \pmod{6}$ and $C_3 \equiv 2 \pmod{3}$,
 - 3. $k \equiv 2 \pmod{3}$
 - (a) $v_3(C) \equiv 0 \pmod{6}$
 - i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
 - ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
 - iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
 - (b) $v_3(C) \equiv 1 \pmod{6}$
 - i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,
 - ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
 - iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,
 - (c) $v_3(C) \equiv 3 \pmod{6}$
 - i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
 - ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
 - iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
 - (d) $v_3(C) \equiv 4 \pmod{6}$
 - i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,
 - ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
 - iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,
- in which case $w_3(t) = (-1)^{v_3(C)+1}$, or else

1. $k \equiv 0 \pmod{3}$,

(a) $v_3(C) \equiv 0 \pmod{6}$

- i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,
- ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
- iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,

(b) $v_3(C) \equiv 2 \pmod{6}$

- i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,
- ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
- iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,

(c) $v_3(C) \equiv 3 \pmod{6}$

- i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,
- ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
- iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,

(d) $v_3(C) \equiv 5 \pmod{6}$

- i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 7 \pmod{9}$,
- ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 4 \pmod{9}$,
- iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 1 \pmod{9}$,

2. $k \equiv 1 \pmod{3}$,

(a) $v_3(C) \equiv 0 \pmod{6}$

- i. $C_3 \equiv 1 \pmod{9}$. $A'^2 \equiv 1, 4 \pmod{9}$ and $B'^2 \equiv 7 \pmod{9}$,
- ii. $C_3 \equiv 2 \pmod{9}$. $A'^2 \equiv 1, 4 \pmod{9}$ and $B'^2 \equiv 7 \pmod{9}$,
- iii. $C_3 \equiv 4 \pmod{9}$. $A'^2 \equiv 1, 7 \pmod{9}$ and $B'^2 \equiv 4 \pmod{9}$,
- iv. $C_3 \equiv 5 \pmod{9}$. $A'^2 \equiv 4, 7 \pmod{9}$ and $B'^2 \equiv 1 \pmod{9}$,
- v. $C_3 \equiv 7 \pmod{9}$. $A'^2 \equiv 4, 7 \pmod{9}$ and $B'^2 \equiv 1 \pmod{9}$,
- vi. $C_3 \equiv 8 \pmod{9}$. $A'^2 \equiv 1, 7 \pmod{9}$ and $B'^2 \equiv 4 \pmod{9}$,

(b) $v_3(C) \equiv 1, 2 \pmod{6}$ and $C_3 \equiv 2 \pmod{3}$,

(c) $v_3(C) \equiv 3 \pmod{6}$

- i. $C_3 \equiv 1 \pmod{9}$. $A'^2 \equiv 4 \pmod{9}$ and $B'^2 \equiv 1, 4 \pmod{9}$,
- ii. $C_3 \equiv 2 \pmod{9}$. $A'^2 \equiv 1 \pmod{9}$ and $B'^2 \equiv 1, 4 \pmod{9}$,
- iii. $C_3 \equiv 4 \pmod{9}$. $A'^2 \equiv 1 \pmod{9}$ and $B'^2 \equiv 1, 7 \pmod{9}$,
- iv. $C_3 \equiv 5 \pmod{9}$. $A'^2 \equiv 4 \pmod{9}$ and $B'^2 \equiv 4, 7 \pmod{9}$,
- v. $C_3 \equiv 7 \pmod{9}$. $A'^2 \equiv 7 \pmod{9}$ and $B'^2 \equiv 4, 7 \pmod{9}$,
- vi. $C_3 \equiv 8 \pmod{9}$. $A'^2 \equiv 7 \pmod{9}$ and $B'^2 \equiv 1, 7 \pmod{9}$,

(d) $v_3(C) \equiv 4, 5 \pmod{6}$ and $C_3 \equiv 2 \pmod{3}$,

3. $k \equiv 2 \pmod{3}$

(a) $v_3(C) \equiv 0 \pmod{6}$

- i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2, 8 \pmod{9}$,
- ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 2, 5 \pmod{9}$,
- iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 5, 8 \pmod{9}$,

(b) $v_3(C) \equiv 1 \pmod{6}$

- i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5 \pmod{9}$,
- ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 8 \pmod{9}$,
- iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 2 \pmod{9}$,

(c) $v_3(C) \equiv 3 \pmod{6}$

- i. $B'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 1, 7 \pmod{9}$,
- ii. $B'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 4, 7 \pmod{9}$,
- iii. $B'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 1, 4 \pmod{9}$,

(d) $v_3(C) \equiv 4 \pmod{6}$

- i. $A'^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 4 \pmod{9}$,

ii. $A'^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1 \pmod{9}$,

iii. $A'^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 7 \pmod{9}$,

in which case $w_3(t) = (-1)^{v_3(C)}$.

Proof. Let $\delta = C(3A^2m^6 + B^2n^6)$. Suppose that $v_3(A) = k$ and $v_3(B) = 0$. Let (m, n) be a pair of coprime integers such that $6v_3(n) < 2k + 1$. One has $v_3(\delta) \equiv v_3(C) \pmod{6}$ and $\delta_3 \equiv C_3B^2n^6 \pmod{9}$. Running through such pairs (m, n) , the function w_2 is constant:

$$w_3(t) = \begin{cases} (-1)^{v_3(C)+1} & \text{si } v_3(C) \equiv 1, 2 \pmod{6} \text{ and } C_3 \equiv 1 \pmod{3} \\ & \text{and si } v_3(C) \equiv 4, 5 \pmod{6} \text{ and } C_3 \equiv 2 \pmod{3}, \\ & \text{si } v_3(C) \equiv 0 \pmod{6} \text{ and } C_3B^2 \equiv 5, 7 \pmod{9} \\ & \text{si } v_3(C) \equiv 3 \pmod{6} \text{ and } C_3B^2 \equiv 2, 4 \pmod{9} \\ (-1)^{v_3(C)} & \text{otherwise.} \end{cases}$$

Suppose now that $6v_3(n) > 2k + 1$. In this case one has $v_3(\delta) = v_3(C) + 2k + 1$ and $\delta_3 \equiv C_3A_3^2m^4$. As previously, we find that with this choice of (m, n) , the value of w_3 is

$$w_3(t) = \begin{cases} (-1)^{v_3(C)} & \text{if } v_3(C) + 2k \equiv 0, 2 \pmod{6} \text{ and } C_3 \equiv 1 \pmod{3} \\ & \text{and if } v_3(C) + 2k \equiv 3, 4 \pmod{6} \text{ and } C_3 \equiv 2 \pmod{3}, \\ & \text{if } v_3(C) + 2k \equiv 5 \pmod{6} \text{ and } C_3B^2 \equiv 5, 7 \pmod{9} \\ & \text{if } v_3(C) + 2k \equiv 2 \pmod{6} \text{ and } C_3B^2 \equiv 2, 4 \pmod{9} \\ (-1)^{v_3(C)} & \text{otherwise.} \end{cases}$$

Remarking that in the following cases we have $C_3B^2 \equiv 5, 7 \pmod{9}$:

1. $B^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 5, 7 \pmod{9}$
2. $B^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 4, 8 \pmod{9}$
3. $B^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 1, 2 \pmod{9}$

and that $C_3B^2 \equiv 2, 4 \pmod{9}$ in the following cases:

1. $B^2 \equiv 1 \pmod{9}$ and $C_3 \equiv 2, 4 \pmod{9}$
2. $B^2 \equiv 4 \pmod{9}$ and $C_3 \equiv 1, 5 \pmod{9}$
3. $B^2 \equiv 7 \pmod{9}$ and $C_3 \equiv 7, 8 \pmod{9}$

we deduce that the function w_3 is constant in the cases listed in the lemma (and only in those cases). To achieve this, we compare the two formulas for each value of $k \pmod{3}$.

When $v_2(A) = 0$ and $v_2(B) = l$, we proceed in a similar way to obtain the previous conditions (where $k = l - 1$ and interchanging A and B) for the function w_3 to be constant. \square

6.3 Local root number at 2

Lemma 6.3. *Let \mathcal{E} be an elliptic surface given by the Weierstrass equation*

$$\mathcal{E} : y^2 = x^3 + C(3A^2T^6 + B^2)x,$$

where $A, B, C \in \mathbb{Z}$ and $\text{pgcd}(A, B) = 1$. For $t = \frac{u}{v} \in \mathbb{Q}$, put $\delta = C(A^2u^4 + B^2v^4)$. We note δ_2 the integer such that $\delta = 2^{\text{ord}_2 \delta} \delta_2$.

The value of the function $w_2(t) := W_2(\mathcal{E}_t) \left(\frac{-1}{\delta_2} \right)$ is constant, equal to $\left(\frac{-1}{C_2} \right)$, when $t \in \mathbb{Q}$ varies if and only if one of the following option is satisfied:

1. $v_2(A)$ and $v_2(B) \equiv 0 \pmod{3}$ and $v_2(C) \equiv 0 \pmod{6}$
2. $v_2(A) \equiv 1 \pmod{3}$ et
 - (a) $v_2(C) \equiv 0 \pmod{6}$
 - (b) $v_2(C) \equiv 2 \pmod{6}$ and $C_2 \equiv 1 \pmod{4}$
 - (c) $v_2(C) \equiv 4 \pmod{6}$ and $C_2 \equiv 3 \pmod{4}$
3. $v_2(B) \equiv 1 \pmod{3}$ and
 - (a) $v_2(C) \equiv 0 \pmod{6}$
 - (b) $v_2(C) \equiv 2 \pmod{6}$ and $C_2 \equiv 3 \pmod{4}$
 - (c) $v_2(C) \equiv 4 \pmod{6}$ and $C_2 \equiv 1 \pmod{4}$
4. $v_2(A) \equiv 2 \pmod{3}$ and

- (a) $v_2(C) \equiv 0 \pmod 6$ and $C_2 \equiv 1 \pmod 4$
- (b) $v_2(C) \equiv 2 \pmod 6$
- (c) $v_2(C) \equiv 4 \pmod 6$ and $C_2 \equiv 3 \pmod 4$
- 5. $v_2(B) \equiv 2 \pmod 3$ and
 - (a) $v_2(C) \equiv 0 \pmod 6$ and $C_2 \equiv 3 \pmod 4$
 - (b) $v_2(C) \equiv 2 \pmod 6$
 - (c) $v_2(C) \equiv 4 \pmod 6$ and $C_2 \equiv 1 \pmod 4$

Proof. Suppose $v_2(A) = k \in \mathbb{N}$ and $v_2(B) = 0$.

Let (m, n) be a pair of coprime integers.

If $6v_2(n) < 2k$, then $v_2(\delta) \equiv v_2(C) \pmod 6$ and $\delta_3 \equiv C_2 \pmod 4$. We have thus

$$w_2(t) = \begin{cases} \left(\frac{-1}{C_2}\right) & \text{if } v_2(C\delta) \equiv 1, 3, 4, 5 \pmod 6 \text{ and } C_2 \equiv 1 \pmod 4 \\ -\left(\frac{-1}{C_2}\right) & \text{if } v_2(C\delta) \equiv 0, 2 \\ \text{or if } v_2(C\delta) \equiv 1, 3, 4, 5 \pmod 6 \text{ and } C_2 \equiv 3 \pmod 4 \end{cases}$$

Remark that this formula also apply to the pairs $(m, n) \in \mathbb{Z}^2$ such that $2 \mid m$.

If $6v_2(n) \geq 2k$, then $v_2(\delta) \equiv v_2(C) + 2k \pmod 6$ and $\delta_2 \equiv 3C_2 \pmod 4$. We have thus

$$w_2(t) = \begin{cases} \left(\frac{-1}{C_2}\right) & \text{if } v_2(C\delta) + 2k \equiv 1, 3, 4, 5 \pmod 6 \text{ and } C_2 \equiv 3 \pmod 4 \\ -\left(\frac{-1}{C_2}\right) & \text{if } v_2(C\delta) + 2k \equiv 0, 2 \\ \text{or if } v_2(C\delta) \equiv 1, 3, 4, 5 \pmod 6 \text{ and } C_2 \equiv 1 \pmod 4 \end{cases}$$

From these formulas, we deduce the following behavior of the function $w_2(t)$ when $6v_2(n) \neq 2k$.

When k is divisible by 3, then the function w_2 is constant equal to $-\left(\frac{-1}{C_2}\right)$ if $v_2(C) = 0, 2 \pmod 6$.

When $k \equiv 1 \pmod 3$, then the function w_2 is constant equal to $-\left(\frac{-1}{C_2}\right)$ if and only if the surface is among the following cases:

1. $v_2(C) \equiv 0 \pmod 6$
2. $v_2(C) \equiv 2 \pmod 6$ and $C_2 \equiv 1 \pmod 4$
3. $v_2(C) \equiv 4 \pmod 6$ and $C_2 \equiv 3 \pmod 4$

When $k \equiv 2 \pmod 3$, then the function w_2 is constant equal to $-\left(\frac{-1}{C_2}\right)$ if and only if the surface is among the following cases:

1. $v_2(C) \equiv 0 \pmod 6$ and $C_2 \equiv 1 \pmod 4$
2. $v_2(C) \equiv 2 \pmod 6$
3. $v_2(C) \equiv 4 \pmod 6$ and $C_2 \equiv 3 \pmod 4$

When $k \equiv 0 \pmod 3$, we need to proceed to a more refined selection, because it is possible that the root number varies when we consider also the integers n such that $6v_2(n) = 2k$. When having a pair (m, n) with a such n , then $v_2(C\delta) = v_2(C) + 2$. Remark that replacing n_2 by n' such that $n' \equiv n_2 + 8 \pmod{16}$, then the value of $\delta_2 \pmod 4$ passes from C_2 to $3C_2$ and vice-versa. Therefore, the local root number varies when we take n such that $6v_2(n) = 2k$ in the case where $v_2(C) \equiv 1, 2, 3, 5 \pmod 6$. It is constant for such pairs when $v_2(C) \equiv 0, 4 \pmod 6$.

Therefore, when $3 \mid k$, the local root number is constant if and only if $v_2(C) \equiv 0 \pmod 6$

Suppose now that $v_2(A) = 0$ and $v_2(B) = k$. Then by a similar argument as previously, we find that $w_2(t)$ is constant and equal to $-\left(\frac{-1}{C_2}\right)$ if and only if

1. $k \equiv 0 \pmod 3$ and $v_2(C) \equiv 0 \pmod 6$
2. $k \equiv 1 \pmod 3$ and
 - (a) $v_2(C) \equiv 0 \pmod 6$
 - (b) $v_2(C) \equiv 2 \pmod 6$ and $C_2 \equiv 3 \pmod 4$
 - (c) $v_2(C) \equiv 4 \pmod 6$ and $C_2 \equiv 1 \pmod 4$
3. $k \equiv 2 \pmod 3$ and
 - (a) $v_2(C) \equiv 0 \pmod 6$ and $C_2 \equiv 3 \pmod 4$
 - (b) $v_2(C) \equiv 2 \pmod 6$
 - (c) $v_2(C) \equiv 4 \pmod 6$ and $C_2 \equiv 1 \pmod 4$

□

6.4 Proof of the Theorem 6.1

Put $C = \text{pgcd}(A, B)$. If $3A/B$ is not a rational square, then by [VA11, Thm 2.1] the root number varies. Suppose thus $3A/B$ is a rational square, that is to say there exists $a, b \in \mathbb{Z}$ such that $3a^2 = \frac{A}{C}$ and $b^2 = \frac{B}{C}$. Let $\mathcal{E} : y^2 = x^3 + C(3A^2m^6 + B^2n^6)$, be the fiber at $t = (m, n) \in \mathbb{P}^1$ associated to X a del Pezzo surface represented in $\mathbb{P}(1, 1, 2, 3)$ be the equation $w^2 = z^3 + Ax^6 + By^6$. Put

$$\delta = c(3a^2m^6 + b^2n^6) = 2^{v_2(\delta)}3^{v_3(\delta)}p_1^{e_1} \dots p_n^{e_n} = 2^{v_2(\delta)}3^{v_3(\delta)}d_1(d_2)^2$$

where $d_1 = \prod_{e_i \text{ impair}} p_i^{e_i}$ and $d_2 = \prod_{e_i \text{ pair}} p_i^{e_i/2}$. As \mathcal{E} is of the form $E_\delta : y^2 = x^3 + \delta$, the root number can be written as

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{d_1}\right)\left(\frac{-3}{d_2}\right).$$

Remark that we have $\left(\frac{-1}{d_1}\right) = \left(\frac{-1}{\delta_2}\right)(-1)^{v_3(\delta)}$, where δ_2 is the integer such that $\delta = 2^{v_2(\delta)}\delta_2$. Thereafter, we will use the following notations:

$$\mathcal{P}(t) := \left(\frac{-3}{d_2}\right), \quad w_2(t) := W_2(E_\delta)\left(\frac{-1}{\delta_2}\right) \quad \text{and} \quad w_3(t) := W_3(E_\delta)(-1)^{v_3(\delta)}.$$

We study the variation of \mathcal{P} , w_2 and w_3 (as the values of those different parts of the root number formula) according to the 2- and 3-adic valuations of a , b and c , the values of $c_2 \bmod 4$ and $c_3 \bmod 9$ and the factorisation in prime numbers of c . The aim is determining the cases where these functions are constant. This will give the global behavior of the root number function.

First, note that for any choice of a , b and c , $\mathcal{P}(t)$ is a constant. It is equal to $\mathcal{P} = (-1)^\sigma$, where

$$\sigma = \#\{p \text{ such that } p^2 | C \text{ and } p \equiv 2 \pmod{3}\},$$

Indeed, the conditions determining the local root number at 3 involve $v_3(\delta) \bmod 6$, and $\delta_3 \bmod 9$, while those determining the local root number at 2 involve $v_2(\delta) \bmod 4$ and $\delta_2 \bmod 4$. Therefore, if one of the values w_2 or w_3 varies, then the global root number is not constant. In the case where one of w_2 or w_3 is fixed and the other varies, there is necessarily a variation of the root number. Moreover, when the two values varies, these variations can not happen always at the same time (and thus the elliptic surface can not have a constant root number in this case).

Therefore, the root number varies, except for the surfaces such that A, B, C fulfil one of the conditions of Lemma 6.3, and one of Lemma 6.2.

Remark 4. The independance of w_2 and of w_3 that we mentionned at the end of the proof is also given by the Helfgott's formula for the average root number [Hel03, Proposition 7.2].

Remark 5. We chose to study a surface given by an equation of the form

$$y^2 = x^3 + AT^6 + B$$

as a sequel of [VA11, Theorem 2.1] which shows that the variation of the root number of the fibers of a rational elliptic surface of the form

$$y^2 = x^3 + F(T)$$

where F has a primitive factor f_i such that $\mu_3 \not\subseteq \mathbb{Q}[T]/f_i$ where μ_3 is the group of the third roots of unity. The most natural counter-example to this property is

$$F(T) = C(3A^2T^6 + B^2).$$

Theorem 6.1 is the natural continuation of the work of Várilly-Alvarado, in particular [VA11, Theorem 1.1].

7 Root number on the fibers of IRES with $j(T) = 1728$

7.1 Necessary and sufficient condition for a constant root numbers

The density of rational points on certain elliptic surfaces of the form $\mathcal{E} : y^2 = x^3 + g(T)x$ is guaranteed by the construction of a section for \mathcal{E} done in part 5.1. However, there are surfaces such that this section is not of infinite order. This happens in particular when $g(T) = AT^4 + B$. In the following, we find as previously which are the rational elliptic surfaces of this form such that the root number of their fiber is constant.

Theorem 7.1. *Let \mathcal{E} be an elliptic surface represented by the Weierstrass equation*

$$\mathcal{E} : y^2 = x^3 + C(A^2T^4 + B^2)x,$$

where $A, B, C \in \mathbb{Z}$ and $(A, B) = 1$.

Then the root number function is constant if and only if $v_3(AB)$ is even and if one of the option of the following list holds:

1. (a) *k is odd*
 - i. $v_2(C) \equiv 0 \pmod{4}$
 - A. $C_2 \equiv 3 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - B. $C_2 \equiv 11 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$
 - ii. $v_2(C) \equiv 1, 3 \pmod{4}$
 - A. $C_2 \equiv 3 \pmod{16},$
 - iii. $v_2(C) \equiv 2 \pmod{4}$ and
 - A. $C_2 \equiv 9 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$
- (b) *k is even and*
 - i. $v_2(C) \equiv 0 \pmod{4}$
 - A. $C_2 \equiv 5, 13 \pmod{16}$
 - B. $C_2 \equiv 7 \pmod{16}, B^2 \equiv A^2 \equiv 9 \pmod{16}$
 - C. $C_2 \equiv 15 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - ii. $v_2(C) \equiv 2 \pmod{4}$ and
 - A. $C_2 \equiv 7, 15 \pmod{16}$
 - B. $C_2 \equiv 5 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - C. $C_2 \equiv 13 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$
2. (a) *k is odd*
 - i. $v_2(C) \equiv 0 \pmod{4}$
 - A. $C_2 \equiv 7 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - B. $C_2 \equiv 15 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$
 - ii. $v_2(C) \equiv 1, 3 \pmod{4}$
 - A. $C_2 \equiv 7 \pmod{16},$
 - iii. $v_2(C) \equiv 2 \pmod{4}$ and
 - A. $C_2 \equiv 5, 7 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
- (b) *k is even and*
 - i. *If $v_2(C) = 0, 2$*
 - A. $C_2 \equiv 7 \pmod{8}$ and $A^2 \equiv B^2 \equiv 9 \pmod{16}$
 - ii. $v_2(C) = 1$
 - A. $C_2 \equiv 7, 15 \pmod{16}$ and $A^2 \equiv B^2 + 8 \pmod{16},$
 - iii. $v_2(C) = 3$
 - A. $C_2 \equiv 5 \pmod{8}$ and $A^2 \equiv B^2 + 8 \pmod{16},$
- (c) *k is odd and*
 - i. $v_2(C) \equiv 0 \pmod{4}$
 - A. $C_2 \equiv 1, 9 \pmod{16}$
 - B. $C_2 \equiv 3 \pmod{16}, B^2 \equiv A^2 \equiv 9 \pmod{16}$
 - C. $C_2 \equiv 11 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - ii. $v_2(C) \equiv 1, 3 \pmod{4}$
 - A. $C_2 \equiv 1, 3 \pmod{8}$
 - iii. $v_2(C) \equiv 2 \pmod{4}$ and
 - A. $C_2 \equiv 3, 11 \pmod{16}$
 - B. $C_2 \equiv 1 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - C. $C_2 \equiv 9 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$
- (d) *k is even and*

- i. If $v_2(C) = 0$
 - A. $C_2 \equiv 1 \pmod{16}$ and $B^2 \equiv 1 \pmod{16}$
 - B. $C_2 \equiv 3 \pmod{16}$ and $A^2 \equiv 9 \pmod{16}$
 - C. $C_2 \equiv 9 \pmod{16}$ and $B^2 \equiv 9 \pmod{16}$
 - D. $C_2 \equiv 11 \pmod{16}$ and $A^2 \equiv 1 \pmod{16}$
- ii. $v_2(C) = 1$
 - A. $C_2 \equiv 3, 11 \pmod{16}$ and $A^2 \equiv B^2 \pmod{16}$
- iii. If $v_2(C) = 2$
 - A. $C_2 \equiv 1 \pmod{16}$ and $A^2 \equiv 1 \pmod{16}$,
 - B. $C_2 \equiv 3 \pmod{16}$ and $B^2 \equiv 9 \pmod{16}$,
 - C. $C_2 \equiv 9 \pmod{16}$ and $A^2 \equiv 9 \pmod{16}$,
 - D. $C_2 \equiv 11 \pmod{16}$ and $B^2 \equiv 1 \pmod{16}$,
- iv. si $v_2(C) = 3$
 - A. $C_2 \equiv 1 \pmod{8}$ and $A^2 \equiv B^2 \pmod{16}$

Put $\sigma = \#\{p \text{ prime number} \mid p^2 \mid C \text{ and } p \equiv 2 \pmod{3}\}$.
The value of the root number on every fiber is

$$W(\mathcal{E}_t) = +1$$

if and only if

- 1. σ is even,
 - (a) $v_3(C) \equiv 2 \pmod{4}$ and the coefficients are as in an option of the list 1
 - (b) $v_3(C) \not\equiv 2 \pmod{4}$ and the coefficients are as in an option of the list 2
- 2. σ is odd
 - (a) $v_3(C) \equiv 2 \pmod{4}$ and the coefficients are as in an option of the list 2
 - (b) $v_3(C) \not\equiv 2 \pmod{4}$ and the coefficients are as in an option of the list 1

Example 3. The surface

$$\mathcal{E} : y^2 = x^3 + 7(9T^4 + 25)x$$

has root number equal to -1 on every fiber at $t \in \mathbb{Q}$.

The surface

$$\mathcal{E} : y^2 = x^3 + 11(9T^4 + 25)x,$$

has root number equal to $+1$ for every fiber at $t \in \mathbb{Q}$.

7.2 Local root number at 3

Lemma 7.2. Let \mathcal{E} be an elliptic surface given by the Weierstrass equation

$$\mathcal{E} : y^2 = x^3 + C(A^2T^4 + B^2)x,$$

where $A, B, C \in \mathbb{Z}$ and $(A, B) = 1$.

The local root number at 3 is constant if and only if $v_3(AB)$ is even. In this case, we have

$$W_3(\delta) = \begin{cases} -1 & \text{if } v_3(C) \equiv 2 \pmod{4} \\ +1 & \text{otherwise.} \end{cases}$$

Proof. Recall the formula in this case (see [VA11, Lemme 4.7]) :

$$W_3(\delta) = \begin{cases} -1 & \text{if } v_3(\delta) \equiv 2 \pmod{4} \\ +1 & \text{otherwise} \end{cases}$$

For each fiber \mathcal{E}_t , we study instead the curve $\mathcal{E}_{m,n} : y^2 = x^3 + C(A^2m^4 + B^2n^4)x$ which is \mathbb{Q} -isomorphic. Put $\delta(m, n) = A^2m^4 + B^2n^4$. The local root number at 3 of $\mathcal{E}_{m,n}$ only depends of $v_3(C\delta(m, n))$. As $v_3(C)$ is fixed, we will study the variation of $v_3(\delta(m, n))$ depending on A and B .

For every $l \in \mathbb{Z}$, we denote by l_3 , the integer such that $l = 3^{v_3(l)}l_3$.

Since by assumption A and B are coprime, this means that 3 can divide at most one of $v_3(A)$ or $v_3(B)$ at a time. We can assume that $3 \nmid B$ and $v_3(A) = k$ for some $k \in \mathbb{Z}$ (otherwise, we interchange the role of A and B). For every $m, n \in \mathbb{Z}$ coprime, we have $\delta(m, n) = 3^{2k+4v_3(m)}A_3^2m_3^4 + B^23^{4v_3(n)}n_3^4$.

In the case where $v_3(n) = 0$, we have $\delta(m, n) \equiv 1 \pmod{4}$ and $v_3(\delta) = 0$. In the case where $0 < v_3(n) \leq \frac{k}{2} - 1$, we have $\delta(m, n)_3 \equiv 3^{2k-4v_3(n)} + 1 \equiv 1 \pmod{3}$ and $v_3(\delta) \equiv 2k - 4v_3(n) \equiv k \pmod{4}$. In the case where $v_3(n) = \frac{k}{2}$ (this only happens if $k \equiv 0, 2 \pmod{4}$), we have $v_3(\delta) \equiv 2k \pmod{4}$ and $\delta_3 \equiv 2 \pmod{4}$. In the case where $v_3(n) \geq \frac{k}{2} + 1$, we have $v_3(\delta) \equiv -2k \pmod{4}$ and $\delta_3 \equiv 1 \pmod{3}$.

Suppose $v_3(AB)$ is odd. Let $m_1, n_1 \in \mathbb{Z}$ be coprime and not divisible by 3. We have $\delta(m_1, n_1) \equiv 0 \pmod{4}$. Let $m, n \in \mathbb{Z}$ be coprime integers such that $3 \mid n$. We have $\delta(m_2, n_2) \equiv 2 \pmod{4}$. Therefore, we have

$$W(\mathcal{E}_{m_1, n_1}) = -W(\mathcal{E}_{m_2, n_2}).$$

Suppose $v_3(AB)$ is even. Then $2k \equiv -2k \equiv 0 \pmod{4}$. Therefore, $v_3(\delta(m, n))$ is constant for any value of $m, n \in \mathbb{Z}$ coprime. We have in this case:

$$W(\mathcal{E}_{m, n}) = -1 \Leftrightarrow v_3(C) \equiv 2 \pmod{4}.$$

□

7.3 Local root number at 2

Lemma 7.3. *Let $A, B, C \in \mathbb{Z}$ be coprime integer such that $2 \nmid B$. Let \mathcal{E} be an elliptic surface given by the Weierstrass equation*

$$\mathcal{E} : y^2 = x^3 + C(A^2T^4 + B^2)x.$$

For $t = \frac{u}{v} \in \mathbb{Q}$, put $\delta = C(A^2u^4 + B^2v^4)$. We denote by δ_2 the integer such that $\delta = 2^{\text{ord}_2 \delta} \delta_2$. If $v_2(A) = 0$, put $k = v_2(B)$ and $A' = B_3$ and $B' = A_3$. Otherwise, put $k = v_2(A)$ and $A' = A_3$ and $B' = B_3$.

The value of $w_2(\mathcal{E}_t) := W_2(\mathcal{E}_t) \left(\frac{-2}{\delta_2} \right)$ is constant when $t \in \mathbb{Q}$ varies if and only if

1. *k is odd*

(a) $v_2(C) \equiv 0 \pmod{4}$

i. $C_2 \equiv 3, 7 \pmod{16}$, $A^2 \equiv B^2 \equiv 1 \pmod{16}$

ii. $C_2 \equiv 11, 15 \pmod{16}$, $A^2 \equiv B^2 \equiv 9 \pmod{16}$

(b) $v_2(C) \equiv 1, 3 \pmod{4}$

i. $C_2 \equiv 3, 7 \pmod{16}$,

(c) $v_2(C) \equiv 2 \pmod{4}$ and

i. $C_2 \equiv 5, 7 \pmod{16}$, $A^2 \equiv B^2 \equiv 1 \pmod{16}$

ii. $C_2 \equiv 9, 13 \pmod{16}$, $A^2 \equiv B^2 \equiv 9 \pmod{16}$

2. *k is even and*

(a) $v_2(C) = 0, 2$

i. $C_2 \equiv 7 \pmod{8}$ and $A^2 \equiv B^2 \equiv 9 \pmod{16}$

(b) $v_2(C) = 1$

i. $C_2 \equiv 7, 15 \pmod{16}$ and $A^2 \equiv B^2 + 8 \pmod{16}$,

(c) $v_2(C) = 3$

i. $C_2 \equiv 5 \pmod{8}$ and $A^2 \equiv B^2 + 8 \pmod{16}$,

in such case $w_2(\mathcal{E}_t) = \left(\frac{-2}{C_2} \right)$; or if:

1. *k is odd and*

(a) $v_2(C) \equiv 0 \pmod{4}$

i. $C_2 \equiv 1, 5, 9, 13 \pmod{16}$

ii. $C_2 \equiv 3, 7 \pmod{16}$, $B^2 \equiv A^2 \equiv 9 \pmod{16}$

iii. $C_2 \equiv 11, 15 \pmod{16}$, $A^2 \equiv B^2 \equiv 1 \pmod{16}$

(b) $v_2(C) \equiv 1, 3 \pmod{4}$

i. $C_2 \equiv 1, 3 \pmod{8}$

(c) $v_2(C) \equiv 2 \pmod{4}$ and

i. $C_2 \equiv 3, 7, 11, 15 \pmod{16}$

ii. $C_2 \equiv 1, 5 \pmod{16}$, $A^2 \equiv B^2 \equiv 1 \pmod{16}$

iii. $C_2 \equiv 9, 13 \pmod{16}$, $A^2 \equiv B^2 \equiv 9 \pmod{16}$

2. *k is even and*

- (a) $v_2(C) = 0$
- i. $C_2 \equiv 1 \pmod{16}$ and $B^2 \equiv 1 \pmod{16}$
 - ii. $C_2 \equiv 3 \pmod{16}$ and $A^2 \equiv 9 \pmod{16}$
 - iii. $C_2 \equiv 9 \pmod{16}$ and $B^2 \equiv 9 \pmod{16}$
 - iv. $C_2 \equiv 11 \pmod{16}$ and $A^2 \equiv 1 \pmod{16}$
- (b) $v_2(C) = 1$
- i. $C_2 \equiv 3, 11 \pmod{16}$ and $A^2 \equiv B^2 \pmod{16}$
- (c) $v_2(C) = 2$
- i. $C_2 \equiv 1 \pmod{16}$ and $A^2 \equiv 1 \pmod{16}$,
 - ii. $C_2 \equiv 3 \pmod{16}$ and $B^2 \equiv 9 \pmod{16}$,
 - iii. $C_2 \equiv 9 \pmod{16}$ and $A^2 \equiv 9 \pmod{16}$,
 - iv. $C_2 \equiv 11 \pmod{16}$ and $B^2 \equiv 1 \pmod{16}$,
- (d) $v_2(C) = 3$
- i. $C_2 \equiv 1 \pmod{8}$ and $A^2 \equiv B^2 \pmod{16}$

in which case $w_2(\mathcal{E}_t) = -\left(\frac{-2}{C_2}\right)$.

Proof. For every choice of $m, n \in \mathbb{Z}$ coprime, let $\mathcal{E}_{m,n} : y^2 = x^3 + C(A^2m^4 + B^2n^4)x$ be an elliptic curve \mathbb{Q} -isomorphic to $E_{\frac{m}{n}}$. We know the formula of the local root number at 2 by [VA11, Lemme 4.7] (that we recall at Lemma 3.2). Moreover, recall that if t is an odd integer, one has

$$\left(\frac{-2}{t}\right) = \begin{cases} +1 & \text{si } t \equiv 1, 3 \pmod{8}, \\ -1 & \text{sinon.} \end{cases}$$

Put, for every $m, n \in \mathbb{Z}$ coprime integers, the integer $\alpha(m, n) = A^2m^4 + B^2n^4$, i.e. $\delta(m, n) = C \cdot \alpha(m, n)$. We study the values of $v_2(\delta)$ and $\delta_2 \pmod{16}$. We will deduce the value of w_2 in each case.

As we supposed that A and B are coprime, there can be only one of them which is not divisible by 2. We can suppose that $v_2(B) = 0$ and that $v_2(A) = k$ where $k \in \mathbb{Z}$ (if it is not the case, we just swap the roles of A and B).

We write

$$\alpha(m, n) = 2^{2k} A_2^2 m^4 + B^2 2^{4v_2(n)} n_2^4,$$

where (m, n) is a pair of coprime integers.

Suppose $2k > 4v_2(n)$. In this case, $v_2(\delta(m, n)) = 4v_2(n) + v_2(C) \equiv v_2(C) \pmod{4}$ and $\delta(m, n)_2 \equiv B^2 C_2 \pmod{16}$. We have,

$$W_2(\mathcal{E}_{m,n}) = \begin{cases} +1 & \text{if } v_2(C) \equiv 0 \pmod{4} \text{ and } B^2 C_2 \equiv 3, 7 \pmod{16}, \\ & \text{if } v_2(C) \equiv 2 \pmod{4} \text{ and } B^2 C_2 \equiv 9, 13 \pmod{16}, \\ & \text{if } v_2(C) \equiv 1, 3 \pmod{4} \text{ and } B^2 C_2 \equiv 5, 7 \pmod{8}, \\ -1 & \text{otherwise.} \end{cases} \quad (5)$$

Suppose $2k < 4v_2(n)$. In this case, $v_2(\delta(m, n)) = 2k + v_2(C) \pmod{4}$. We have $\delta_2 \equiv C_2 A_2^2 \pmod{16}$. Therefore, the root number is

$$W_2(\mathcal{E}_{m,n}) = \begin{cases} +1 & \text{if } v_2(C) \equiv 2k \pmod{4} \text{ and } C_2 A_2^2 \equiv 3, 7 \pmod{16}, \\ & \text{if } v_2(C) \equiv 2k - 2 \pmod{4} \text{ and } C_2 A_2^2 \equiv 9, 13 \pmod{16}, \\ & \text{if } v_2(C) \equiv 1, 3 \pmod{4} \text{ and } C_2 A_2^2 \equiv 5, 7 \pmod{8}, \\ -1 & \text{otherwise.} \end{cases} \quad (6)$$

Suppose k is odd.

Then, if k is odd, then the function w_2 is constant in the following cases :

1. $v_2(C) \equiv 0 \pmod{4}$
 - (a) $C_2 \equiv 3, 7 \pmod{16}$, $A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - (b) $C_2 \equiv 11, 15 \pmod{16}$, $A^2 \equiv B^2 \equiv 9 \pmod{16}$
2. $v_2(C) \equiv 1, 3 \pmod{4}$
 - (a) $C_2 \equiv 3, 7 \pmod{16}$,
3. $v_2(C) \equiv 2 \pmod{4}$ and

- (a) $C_2 \equiv 5, 7 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - (b) $C_2 \equiv 9, 13 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$
- in which case $w_2(t) = \left(\frac{-2}{C_2}\right)$ or else

1. $v_2(C) \equiv 0 \pmod{4}$
 - (a) $C_2 \equiv 1, 5, 9, 13 \pmod{16}$
 - (b) $C_2 \equiv 3, 7 \pmod{16}, B^2 \equiv A^2 \equiv 9 \pmod{16}$
 - (c) $C_2 \equiv 11, 15 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
2. $v_2(C) \equiv 1, 3 \pmod{4}$
 - (a) $C_2 \equiv 1, 3 \pmod{8}$
3. $v_2(C) \equiv 2 \pmod{4}$ and
 - (a) $C_2 \equiv 3, 7, 11, 15 \pmod{16}$
 - (b) $C_2 \equiv 1, 5 \pmod{16}, A^2 \equiv B^2 \equiv 1 \pmod{16}$
 - (c) $C_2 \equiv 9, 13 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$

in which case $w_2 = -\left(\frac{-2}{C_2}\right)$.

Suppose now k is even.

Remark that if $k = 0$, then it is not possible to have $k = 2k > 4v_2(n)$. However, when we take (m, n) a pair of coprime integers such that $2 \mid m$, then we obtain the formula (6).

We find the following cases where the root number is constant when $v_2(n), v_2(m) \neq 2k$.

1. $v_2(C) \equiv 0, 2 \pmod{4}$
 - (a) $C_2 \equiv 7 \pmod{16}, A^2 \equiv B^2 \equiv 9 \pmod{16}$
2. $v_2(C) \equiv 1, 3 \pmod{4}$
 - (a) $C_2 \equiv 5, 7 \pmod{8}$,

in which case $w_2(t) = \left(\frac{-2}{C_2}\right)$ or else

1. $v_2(C) \equiv 0 \pmod{4}$
 - (a) $C_2 \equiv 1, 5 \pmod{16}, B^2 \equiv 1 \pmod{16}$
 - (b) $C_2 \equiv 3, 7 \pmod{16}, A^2 \equiv 9 \pmod{16}$
 - (c) $C_2 \equiv 5 \pmod{16}, B^2 \equiv 1 \pmod{16}$,
 - (d) $C_2 \equiv 9, 13 \pmod{16}, B^2 \equiv 9 \pmod{16}$
 - (e) $C_2 \equiv 11, 15 \pmod{16}, A^2 \equiv 1 \pmod{16}$
2. $v_2(C) \equiv 1, 3 \pmod{4}$
 - (a) $C_2 \equiv 1, 3 \pmod{8}$,
3. $v_2(C) \equiv 2 \pmod{4}$
 - (a) $C_2 \equiv 1, 5 \pmod{16}, A^2 \equiv 1 \pmod{16}$
 - (b) $C_2 \equiv 3, 7 \pmod{16}, B^2 \equiv 9 \pmod{16}$
 - (c) $C_2 \equiv 5 \pmod{16}, A^2 \equiv 1 \pmod{16}$,
 - (d) $C_2 \equiv 9, 13 \pmod{16}, A^2 \equiv 9 \pmod{16}$
 - (e) $C_2 \equiv 11, 15 \pmod{16}, B^2 \equiv 1 \pmod{16}$

in which case $w_2 = -\left(\frac{-2}{C_2}\right)$.

For these exceptions, we proceed to a more raffined sorting.

According to the values of $A^2m^4, B^2n_2^4$ (which are among $1, 9, 17, 25 \pmod{32}$), we find the possible values of δ_2 and $v_2(\delta)$.

In every case, we have $v_2(\delta) = v_2(C) + 2k + 1 \equiv v_2(C) + 1 \pmod{4}$. Remark that m^4 and n_2^4 can take the values $1, 17 \pmod{32}$. Therefore, choosing a value $n'^4 \equiv 17n^4 \pmod{32}$, we have $\delta_2' \equiv 9\delta_2 \pmod{16}$. Therefore, we have (if $A^2 \equiv B^2 \pmod{16}$), $\delta_2 \in \{1, 9 \pmod{16}\}$ and if $A^2 \not\equiv B^2 \pmod{16}$, $\delta_2 \in \{5, 13\}$.

Let t_1, t_5, t_9, t_{13} (if they exist) be the rational numbers associated to a pair of coprime integers (m_i, n_i) such that $\delta_2(m_i, n_i) = i$. The existence of t_1, t_9 holds if and only if $A^2 \equiv B^2 \pmod{16}$ and the existence of t_5, t_{13} if and only if $A^2 \equiv B^2 + 8 \pmod{16}$.

Suppose $v_2(C) = 0, 2$. Then

$$w_2(t^i) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 5, 7 \pmod{8}, \text{ if } i = 1, 9$$

$$w_2(t^i) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 3 \pmod{8}, \text{ if } i = 5, 13.$$

If we compare the behavior of the function w_2 when $4v_2(n) = 2k$ with the one where $4v_2(n) \neq 2k$, we only keep the following cases, on which the root number is constant:

1. If $v_2(C) = 0, 2$

(a) $C_2 \equiv 7 \pmod{8}$ and $A^2 \equiv B^2 \equiv 9 \pmod{16}$

in which case $w_2(\mathcal{E}_t) = \left(\frac{-2}{C_2}\right)$ and the following:

1. If $v_2(C) = 0$

(a) $C_2 \equiv 1 \pmod{16}$ and $B^2 \equiv 1 \pmod{16}$

(b) $C_2 \equiv 3 \pmod{16}$ and $A^2 \equiv 9 \pmod{16}$

(c) $C_2 \equiv 9 \pmod{16}$ and $B^2 \equiv 9 \pmod{16}$

(d) $C_2 \equiv 11 \pmod{16}$ and $A^2 \equiv 1 \pmod{16}$

2. If $v_2(C) = 2$

(a) $C_2 \equiv 1 \pmod{16}$ and $A^2 \equiv 1 \pmod{16}$,

(b) $C_2 \equiv 3 \pmod{16}$ and $B^2 \equiv 9 \pmod{16}$,

(c) $C_2 \equiv 9 \pmod{16}$ and $A^2 \equiv 9 \pmod{16}$,

(d) $C_2 \equiv 11 \pmod{16}$ and $B^2 \equiv 1 \pmod{16}$,

in which case $w_2(\mathcal{E}_t) = -\left(\frac{-2}{C_2}\right)$.

Suppose that $v_2(C) = 1$. Then

$$w_2(t_1) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 9, 13 \pmod{16}$$

$$w_2(t_9) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 5 \pmod{16}$$

$$w_2(t_5) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 3, 7, 11, 13, 15 \pmod{16}$$

$$w_2(t_{13}) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 3, 5, 7, 9, 11, 15 \pmod{16}$$

If we compare the behavior of the function w_2 when $4v_2(n) = 2k$ with the one where $4v_2(n) \neq 2k$, we only keep the following cases, on which the root number is constant for all t :

1. $C_2 \equiv 7, 15 \pmod{16}$ and $A^2 \equiv B^2 + 8 \pmod{16}$,

in which case $w_2(\mathcal{E}_t) = \left(\frac{-2}{C_2}\right)$ and the following:

2. $C_2 \equiv 3, 11 \pmod{16}$ and $A^2 \equiv B^2 \pmod{16}$

in which case $w_2(\mathcal{E}_t) = -\left(\frac{-2}{C_2}\right)$.

Suppose that $v_2(C) = 3$. Then

$$w_2(t_1) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 3, 7 \pmod{16}$$

$$w_2(t_9) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 11, 15 \pmod{16}$$

$$w_2(t_5) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 3, 5, 9, 13, 15 \pmod{16}$$

$$w_2(t_{13}) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 5, 7, 9, 11, 13 \pmod{16}$$

If we compare the behavior of the function w_2 when $4v_2(n) = 2k$ with the one for $4v_2(n) \neq 2k$, we keep only the following cases, on which the root number is constant for all t :

1. $C_2 \equiv 5 \pmod{8}$ and $A^2 \equiv B^2 + 8 \pmod{16}$,

in which case $w_2(\mathcal{E}_t) = \left(\frac{-2}{C_2}\right)$ and the following:

2. $C_2 \equiv 1 \pmod{8}$ and $A^2 \equiv B^2 \pmod{16}$

in which case $w_2(\mathcal{E}_t) = -\left(\frac{-2}{C_2}\right)$. □

7.4 Proof of Theorem 7.1

Let \mathcal{E} be an isotrivial elliptic surface of the form

$$\mathcal{E} : y^2 = x^3 + C^2(A^2m^4 + B^2n^4),$$

where $A, B, C \in \mathbb{Z}$ and $(A, B) = 1$. The root number at t of this surface is given by the formula

$$W(\mathcal{E}_t) = -W_2(\mathcal{E}_t)W_3(\mathcal{E}_t) \left(\frac{-2}{t_1} \right) \left(\frac{-1}{\tau_2} \right),$$

where t_1 and τ_2 are as defined in this theorem. Put $\delta = A^2m^4 + B^2n^4$. Remark that $\left(\frac{-2}{t_1} \right) = \left(\frac{-2}{t'} \right)$, where t' is the integer such that $t' = 2^{v_2(t)}t'$. Hereafter, we will use the following notations: $\mathcal{P}(t) := \left(\frac{-1}{t_2} \right)$, $w_2(t) := W_2(E_\delta) \left(\frac{-2}{t'} \right)$ and $w_3(t) := W_3(E_t)$.

The variation of \mathcal{P} , w_2 and w_3 , the different parts of the formula for the root number, according the 2- and 3-adic valuation of a , b and c , the values of $c_2 \pmod{16}$ and $c_3 \pmod{3}$ and the factorisation in prime numbers of c , allows to distinguish the cases where these components are constant.

First, remark that for all A, B and C , the value of $\mathcal{P}(t)$ is constant on every fibers. Explicitely, we have

$$\mathcal{P} = (-1)^\sigma,$$

where

$$\sigma = \#\{p \text{ such that } p^2 | c \text{ and } p \equiv 3 \pmod{4}\}.$$

Lemma 7.3 gives conditions for w_2 to be constant and Lemma 7.2 gives conditions for W_3 to be constant. Combining those results, we obtain the conditions and conclusion of the theorem.

8 Non-isotrivial rational elliptic surfaces

8.1 Known results

The preprint of Helfgott [Hel03], reviewed in the ph.D thesis of the author [Des16a], proves the following theorem :

Theorem 8.1. *Let \mathcal{E} be a rational elliptic surface given by the equation*

$$\mathcal{E} : y^2 = x^3 + F(u, 1)x + G(u, 1),$$

where F and G are homogeneous polynomials of degree respectively 4 and 6 defining a minimal model. We suppose that \mathcal{E} is non-isotrivial, and thus in particular $FG \neq 0$. Put $\Delta = 4F^3 + 27G^2 = \prod_{i=0}^s P_i^{m_i}$ (the discriminant of \mathcal{E}) and $M_\mathcal{E}(u, v) = \prod_{i \in \mathcal{M}_\mathcal{E}} P_i(u, v)$ where $\mathcal{M}_\mathcal{E} = \{i \text{ such that } P_i \nmid F\}$ (the product of polynomials coming from places of multiplicative reduction).

Suppose that every $P \mid \Delta$ verifies the squarefree conjecture and every $P \mid M_\mathcal{E}$ verifies Chowla's conjecture.

Then the sets W_\pm are both infinite.

The work of Helfgott ([Hel03]) imposes that Δ verifies the squarefree conjecture, and that $M_\mathcal{E}$ verifies Chowla's conjecture. We can use these conjectures under two forms:

- A. the homogeneous version, which holds if
 - (a) $\deg P_i \leq 6$ (squarefree conjecture) and
 - (b) $\deg M_\mathcal{E} \leq 3$ or if $M_\mathcal{E}$ is a product of linear factors (Chowla's conjecture);
- B. the one variable version, which holds if
 - (a) $\deg P_i \leq 3$ (squarefree conjecture) and
 - (b) $\deg M_\mathcal{E} \leq 1$ (Chowla's conjecture).

The following proposition classifies all the rational elliptic surfaces on which the work of Helfgott is unconditional.

Proposition 8.2. *Let \mathcal{E} be a non-isotrivial rational elliptic surface given by the equation:*

$$\mathcal{E} : y^2 = x^3 + F(T, 1)X + G(T, 1),$$

where F and G are homogeneous polynomials of degree respectively 4 and 6.

We suppose that \mathcal{E} respects one of the following properties:

1. $\mathcal{M} = \emptyset$;

2. the places in \mathcal{M} are all rational;
3. $\mathcal{M} = \{P\}$ where $P \in \mathbb{Z}[T]$ is a polynomial of degree 3;
4. $\mathcal{M} = \{P_1, P_2\}$ where $P_1, P_2 \in \mathbb{Z}[T]$ are polynomials of degree respectively 1 and 2;
5. $\mathcal{M} = \{\frac{1}{T}, P_2\}$ where $P_2 \in \mathbb{Z}[T]$ is a polynomial of degree 2.

Then the sets W_{\pm} are both infinite.

Remark 6. There are examples of rational elliptic surfaces of each of the case of the list.

When $\mathcal{M} = \emptyset$, the surface obtained by the contraction of the canonical section never is a del Pezzo surface of degree 1. Indeed, an elliptic surface with no place of multiplicative reduction admits automatically a place of potentially multiplicative reduction. In this case, Corollary 2.3 gives us that \mathcal{E} does not come from a degree 1 del Pezzo surface.

There is del Pezzo surfaces of degree 1 in any other case.

Remark 7. The geometric arguments presented in the section 8.3 prove the density in certain cases on which it is not possible to apply unconditionnally the work of Helfgott.

Proposition 8.5 requires that there exists a rational place of type I_m^* , II^* , III^* , IV^* or I_0^* .

Proof. (of Proposition 8.2)

Let $B_{\mathcal{E}}$ and $M_{\mathcal{E}}$ be the polynomial such that

1. $B_{\mathcal{E}}$ is the product of the polynomial associated to the places of bad reduction of \mathcal{E} that are not of type I_0^* ,
2. $M_{\mathcal{E}}$ the product of the polynomial associated to the places of multiplicative reduction of \mathcal{E} .

Theorem 8.1 and the parity conjecture show the variation of the root number on the fibers when \mathcal{E} is a non-isotrivial surface whose polynomial $B_{\mathcal{E}}$ and $M_{\mathcal{E}}$ are such that

1. $B_{\mathcal{E}}$ verifies the homogeneous version of the squarefree conjecture,
2. $M_{\mathcal{E}}$ verifies the homogeneous version of Chowla's conjecture.

It suffices to verify in which cases these hypothesis hold.

If there exists no place of multiplicative reduction on \mathcal{E} , we have $M_{\mathcal{E}} = 1$. Thus there is no need to consider Chowla's conjecture. Moreover, the irreducible factors of Δ appear with the exponent ≥ 2 . They are of degree ≤ 6 . Therefore, the homogeneous version of squarefree conjecture holds.

Suppose now that \mathcal{E} admits a place of multiplicative reduction on \mathcal{E} .

Let be the following minimal Weierstrass model for \mathcal{E} :

$$y^2 = x^3 + F(T, 1)x + G(T, 1),$$

where $F, G \in \mathbb{Z}[U, V]$ are homogeneous polynomials of degree 4 and 6 respectively. Let C , be the largest primitive polynomial such that $C \mid F$ and $C^2 \mid G$. We write $F = aCF_1$ and $G = bC^2G_1$ where F_1 and G_1 are primitive polynomial and $a, b \in \mathbb{Z}$ are constants. Let $R := \text{pgcd}(F_1, G_1)$. Remark that the polynomial R splits by construction. We write $F = aCRF_2$ and $G = bC^2RG_2$ where $F_2, G_2 \in \mathbb{Z}[X, Y]$ are suitable polynomials. The discriminant can be written

$$\Delta = C^3 R^2 (4a^3 R F_2^3 + 27b^2 C G_2^2).$$

When the surface is non-isotrivial, if there exists P a polynomial such that $P^4 \mid F$, then $P^6 \nmid G$, and thus $\text{ord}_P C \leq 3$. Remark that R, C, F_2 and G_2 verify the homogeneous version of squarefree conjecture as their degrees are ≤ 6 .

We define $M_o = (4RF_2^3 - 27CG_2^2)$ and we remark that $\Delta = C^2 R^3 M_o$. The polynomial M_o is a product of powers of polynomials associated to places of multiplicative or additive reduction. It is possible that M_o is divisible by the polynomials associated to places of additive reduction : the factors of C or R . For $F = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ (the decomposition of F in irreducible factors) there exist integers $\beta_i \in \mathbb{N}$ such that

$$M_1 = \frac{M_o}{P_1^{\beta_1} \dots P_r^{\beta_r}}.$$

□

Lemma 8.3. *Let M be a homogeneous polynomial.*

Then M satisfies the homogeneous version of Chowla's conjecture if

1. *it is a product of linear polynomials ;*
2. *it is a product of a power of a linear polynomial and of an irreducible quadratic polynomial ; or*
3. *it is a polynomial of degree 3.*

8.2 Rational elliptic surfaces with no place of multiplicative reduction

Proposition 8.4. *Let X be a non-isotrivial rational elliptic surface with no place of reduction of type I_m . Then X can be described by one of the following equations:*

$$\mathcal{E}_1 : y^2 = x^3 + aL_1^2Qx + bL_1^3QM, \quad (7)$$

where $Q = \frac{cL_1^2 - 27b^2M^2}{4a^3}$; and

$$\mathcal{E}_2 : y^2 = x^3 + aL_1^2L_2L_3x + bL_1^3L_2^2L_3, \quad (8)$$

where $L_1 = 4a^3L_3 - 27b^2L_2$. We have $a, b \in \mathbb{Z}$, L_1, L_2, L_3 and M linear polynomials and Q a quadratic polynomial.

Remark 8. The homogeneous and one-variable versions of the conjectures hold on the surfaces \mathcal{E}_a and \mathcal{E}_b . Indeed, Chowla's conjecture is true since $M_{\mathcal{E}} = 1$, and as every irreducible factors of the coefficients are linear, squarefree conjecture also holds.

Remark 9. In the first case, the places of bad reduction are those associated to L_1 (of type I_2^*), and those associated to the irreducible factors of Q (of type II).

In the second case, we have three rational places of bad reduction: the one associated to $4a^3L_2 - 27b^2L_3$ has type I_1^* , the one associated to L_2 has type III and the one associated to L_3 has type II .

Proof. Let \mathcal{E} be the rational elliptic surface associated to X , given by the Weierstrass equation:

$$\mathcal{E} : y^2 = x^3 - 27c_4(T)x - 54c_6(T),$$

where $c_4(T), c_6(T) \in \mathbb{Z}[T]$ have degree respectively less than or equal to 4 and 6. Let Δ be the discriminant of \mathcal{E} . This surface has a place of reduction of type I_m^* because the invariant $j = \frac{c_4^3}{\Delta}$ admits necessarily a pole (at a irreducible polynomial $P \in \mathbb{Z}[T]$ or at $\frac{1}{T}$).

Each fiber at $t = \frac{m}{n}$ is given by the equation :

$$\mathcal{E}_t = \mathcal{E}_{m,n} : y^2 = x^3 + n^{4-\deg c_4}c_4\left(\frac{m}{n}\right)x + n^{6-\deg c_6}c_6\left(\frac{m}{n}\right).$$

Suppose the P is the polynomial associated to a place of reduction type I_m^* , then we write $F = P^2F_1$ and $G = P^3G_1$ for F_1, G_1 polynomials. We have that $P \mid (F_1^3 - G_1^2)$. We need to have $\deg P = 1$. Indeed, if $\deg P = 2$, then G_1 and F_1 are constant and thus \mathcal{E} is isotrivial. The case where $\deg P > 2$ is not possible because we would have $\deg G > 6$. Therefore, a non-isotrivial rational elliptic surface with no place of type I_m admits a rational place of reduction I_m^* . We have $\deg P = 1$, $\deg F_1 = 2$ and $\deg G_1 = 3$.

The case where $(F_1, G_1) = 1$ is not possible. Indeed, we would have $P^6 \mid F_1^3 - G_1^2$ and the surface would be isotrivial. Therefore, F_1 and G_1 have a common factor, that we will denote by A . We write $F_1 = AF_2$ and $G_1 = AG_2$ for convenient polynomial F_2 and G_2 . We have $\Delta = P^6A^2(AF_2^3 - G_2^2)$. The reduction at A is thus additive.

Suppose $\deg A = 2$. In this case, if $(A, G_2) = 1$, we have

$$A = \gamma P^2 + G_2^2.$$

If $(A, G_2) = A_2$ for a linear polynomial A_2 , then we have

$$P = \frac{A_1 - A_2}{\gamma}.$$

Suppose $\deg A = 1$. If $A \mid G_2$, we must have

$$A = \frac{F_2^3 - \gamma P^3}{G_2^2}.$$

However, there exist no polynomial $A, P, G_2, F_2 \in \mathbb{Z}[T]$ with this property. Indeed, by imposing a linear change $v = P(t)$, and putting $\nu = \frac{u}{v}$, we are lead to solve

$$4a^3F_2(\nu)^3 + 27b^2A(\nu)M(\nu)^2 = c.$$

As $F_2 \neq P$, $F_2(\nu)$ is non-constant. Let u_0 such that $F_2(u_0) = 0$. We have

$$27b^2A(u_0)G_3(u_0)^2 = c \neq 0.$$

By deriving at u_0 , we obtain :

$$2A(u_0)G_3(u_0)G_3'(u_0) + A'(u_0)G_3(u_0)^2 = 0.$$

When we derive another time, we have :

$$2A(u_0)G'_3(u_0)^2 + 2A(u_0) + 4A'(u_0)G'_3(u_0)G_3(u_0) + A''(u_0)G_3(u_0)^2 = 0.$$

We remark that G_3 is linear. We have:

$$2A(u_0)G'_3(u_0) + 4A'(u_0)G_3(u_0) = 0.$$

Therefore, A is proportionnal to G_3 . For all $P \in \mathbb{Z}[T]$ linear, the polynomial $P(T)^3 - c$ has no double root. Thus, F_2 has to be constant. Therefore G_3, F_2, A and P are proportional to each other and the surface \mathcal{E} is isotrivial.

If $A \nmid G_2$, we must have the equality

$$A = \frac{\gamma P^4 + G_2^2}{F_2^3}.$$

By a similar argument as in the previous case, this is not possible either. \square

8.3 Geometric arguments

In this section we prove unconditionally the density on many more elliptic surfaces, not necessarily isotrivial. Moreover Helfgott's paper does not prove unconditionally the variation of the root number those surfaces.

Proposition 8.5. *Let \mathcal{E} be a elliptic surface given by the equation*

$$\mathcal{E} : y^2 = x^3 + L^2 Qx + L^3 C, \quad (9)$$

where $L, Q, C \in \mathbb{Z}[u, v]$ have respective degree 1, 2 and 3. Then the surface is unirational. In particular, $\mathcal{E}(\mathbb{Q})$ is Zariski-dense.

Remark 10. The polynomial L of the surface \mathcal{E} in this proposition is such that $L^6 \mid \Delta$. As we chose a minimal Weiestrass model for \mathcal{E} , this means that the reduction at L has type I_0^*, II^*, III^*, IV^* or I_m^* . Conversely, if we consider a surface with a rational place of one of these types, we can find an equation of the form (9). We deduce directly the following corollary:

Corollary 8.6. *If a rational elliptic surface \mathcal{E} has a rational place of type I_0^*, II^*, III^*, IV^* or I_m^* , then the rational points of X are Zariski-dense.*

In particular, if \mathcal{E} is a non-isotrivial elliptic surface with no place of multiplicative reduction, then its rational points are dense.

Proof. Let S be an elliptic surface given by the equation

$$S : y^2 = x^3 + L(t, 1)^2 Q(t, 1)x + L(t, 1)^3 C(t, 1),$$

where $L, Q, C \in \mathbb{Z}[u, v]$ have respective degree 1, 2 and 3. Remark that this surface is rational. We study the surface which is birational

$$\left(\frac{y}{L^3}\right)^2 = \left(\frac{x}{L^2}\right)^3 + \frac{Q}{L^2}\left(\frac{x}{L^2}\right) + \left(\frac{C}{L^3}\right). \quad (10)$$

We can suppose that $L(u, v) = v$ (otherwise, we do a linear change on u, v). Put $t = \frac{u}{v}$, $x' = \frac{x}{v^2}$ and $y' = \frac{y}{v^3}$, whose inverse transformation is $x = x'v^2$, $y = y'v^3$, $u = tv$. By this change of variables, (10) becomes

$$S' : y'^2 = x'^3 + q(t)x' + c(t) \subset \mathbb{P}^3,$$

with $Q(t, 1) = q(t)$ and $C(t, 1) = c(t)$, which is a cubic surface with a finite number of singular points.

Remark that on a cubic surface which is not a cone on a cubic curve, the existence of a rational point is equivalent to the density of the rational points. This is shown by Kollar [Kol02], generalizing the work of Segre and Manin [Man74].

From a geometric point of view, this surface is obtained by the contraction of two exceptional curves. For a surface obtained by the successive blow-down of two disjoint exceptional curves (which is the case of S'), we are guaranteed to have a rational point: the one associated to the point $[0, 0, 1, 1]$ (which is not singular). \square

In the previous section, we show that a rational elliptic surface with no place of multiplicative reduction has one of the two following forms:

$$\mathcal{E}_1 : y^2 = x^3 + aL_1^2 Qx + bL_1^3 QM \quad (11)$$

and

$$\mathcal{E}_2 : y^2 = x^3 + a(4a^3L_3 - 27b^2L_2)^2L_2L_3x + b(4a^3L_3 - 27b^2L_2)^3L_2^2L_3, \quad (12)$$

where $a, b \in \mathbb{Z}$, L_1, L_2, L_3 and M linear polynomials and Q a quadratic polynomial. In the first case, we impose moreover that M is such that $M^2 = (\frac{L_1^2 - 4a^3Q}{27b^2})$.

On surface \mathcal{E}_1 , the places of bad reduction are those associated to L_1 , of type I_2^* , and those associated to the irreducible factors of Q , of type II .

On surface \mathcal{E}_2 , we have three rational places of bad reduction - the one associated to $4a^3L_2 + 27b^2L_3$ has type I_1^* , the one associated to L_2 has type III and the one associated to L_3 has II .

Therefore, the results previously presented prove the density of rational points on these surfaces. The work of Helfgott proves in those cases the density of rational points although under the parity conjecture which we are not using here.

There is a fourth method to show the density, at least for surface \mathcal{E}_2 . Let \mathcal{E} be an elliptic surface and E its generic fiber (that is to say \mathcal{E} seen as an elliptic curve over $\mathbb{Q}(T)$). By the Shioda-Tate formula, we have

$$\text{rg}NS(\mathcal{E}_{\overline{\mathbb{Q}}}) = 2 + \text{rg}E(\overline{\mathbb{Q}}(T)) + \sum_v (m_v - 1).$$

The surfaces that we consider are obtained by blowing-up \mathbb{P}^2 at 9 points in general position, the Néron-Severi rank is $\text{rg}NS(\mathcal{E}) = 10$.

In the first case, Shioda-Tate formula says that $\text{rg}E(\overline{\mathbb{Q}}(T)) = 4$. Unfortunately, although it gives an interesting majoration : $\text{rg}(E(\mathbb{Q}(T))) \leq 4$, this is not precise enough to conclude on the density. There is indeed an uncertainty, except in the case where we can bound it this way : $\text{rg}(E(\mathbb{Q}(T))) \geq 1$. It is just what happen in the second case. Indeed the Shioda-Tate formula gives $\text{rg}E(\overline{\mathbb{Q}}(T)) = 1$.

We have $\mathcal{E}(\overline{\mathbb{Q}}(T)) = \mathbb{Z} \cdot P_o$, for a certain point P_o . Therefore there exists K a quadratic extension of \mathbb{Q} such that $P_o \in \mathcal{E}(K(T))$. Indeed, if for every $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$ we put $\sigma P_o := \varepsilon(\sigma) \cdot P_o$ where $\varepsilon : G_{\mathbb{Q}} \rightarrow \pm 1$, then

1. either ε is trivial and $P_o \in E(\mathbb{Q}(T))$,
2. or ε is non-trivial and in this case, $\overline{\mathbb{Q}}^{\text{Ker} \varepsilon} = K$, the subfield of $\overline{\mathbb{Q}}$ stabilised by ε , is a quadratic field such that $P_o \in E(K(T))$.

One can remark, similarly as in the proof of Proposition 8.5, that \mathcal{E}_2 is birational to a cubic surface. We use the following proposition to end the argument :

Proposition 8.7. *Let S be a non-singular cubic surface on a number field k . Suppose S is not a cone on a cubic curve.*

1. *If $S(k) \neq \emptyset$, then $S(k)$ is Zariski-dense.*
2. *Let k_1 be a quadratic extension of k . If $S(k_1) \neq \emptyset$ is Zariski-dense, then $S(k)$ is Zariski-dense.*

Proof. The first statement of the proposition is shown by Segre and Manin (see [Man74]). They actually prove a stronger result : if k is an arbitrary field and that $S(k) \neq \emptyset$, then S est k -unirational. When k is infinite, this implies the Zariski-density of rational points.

We now show the second point of the proposition. Let $P \in S(k_1)$. If $P \in S(k)$, then the rational points are dense. Suppose the that $P \notin S(k)$. Consider D the line passing through P and P^σ where σ is the automorphism of k_1 fixing k . If $D \subset S$, then $D(k) \subset S(k)$ and thus the set of rational points of S is not empty. Otherwise, the intersection $D \cap S$ contains three points : P , P^σ , and a third point which is necessarily in $S(k)$. \square

We end the section with a result concerning smooth rational elliptic surfaces, associated to a del Pezzo surface of degree 1. Let X be a del Pezzo surface of degree 1. In general, if there exists C_1 and C_2 a pair of exceptional curves defined over \mathbb{Q} on X such that their intersection is empty, one can contract those curves to obtain X_3 a del Pezzo surface of degree 3. On X_3 , the existence of a rational point guarantees the Zariski-density of $X(k)$. In what follows, we use this idea to prove the density one some other surfaces on which we find two exceptional curves with non empty intersection.

Proposition 8.8. *Let X a del Pezzo surface of degree 1 on which lie \mathcal{C}_1 and \mathcal{C}_2 two distinct exceptional curves with possibly points in common. Then $X(k)$ is Zariski-dense.*

Proof. The contraction of \mathcal{C} gives X' a del Pezzo surface of degree 2. We know that on these surfaces, the rational points of X' are dense if $X'(k)$ contains a point which is neither on an exceptional curve nor on a distinguished quartic. Put \mathcal{E} the union of the points of this quartic and of the exceptional curves. The contraction sends \mathcal{C}_2 on a rational curve of X' that we will denote by \mathcal{C} . Remark that \mathcal{C} is not an exceptional curve on X' because it is the blow-down of a curve which has a point in common with \mathcal{C}_1 . In the case where $\mathcal{C} \cap \mathcal{E}$ is finite, one can find a rational point outside of \mathcal{E} , and this proves the density of the rational points. \square

References

- [CCH05] B. Conrad, K. Conrad, and H. Helfgott. Root numbers and ranks in positive characteristic. *Adv. Math.*, 198(2):684–731, 2005.
- [CS82] J. W. S. Cassels and A. Schinzel. Selmer’s conjecture and families of elliptic curves. *Bull. London Math. Soc.*, 14(4):345–348, 1982.
- [CT90] Jean-Louis Colliot-Thélène. Surfaces rationnelles fibrées en coniques de degré 4. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 43–55. Birkhäuser Boston, Boston, MA, 1990.
- [Del73] P. Deligne. Les constantes des équations fonctionnelles des fonctions L . In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.
- [Des16a] J. Desjardins. *Densité des points rationnels sur les surfaces elliptiques et les surfaces de del Pezzo de degré 1*. PhD thesis, Université Paris-Diderot - Paris VII, November 2016.
- [Des16b] J. Desjardins. On the variation of the root number of the fibers in families of elliptic curves. Submitted, 2016.
- [Hal98] Emmanuel Halberstadt. Signes locaux des courbes elliptiques en 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 326(9):1047–1052, 1998.
- [Hel03] H. A. Helfgott. On the behaviour of root numbers in families of elliptic curves. arXiv:math/0408141v3, 2003.
- [Isk79] V. A. Iskovskih. Minimal models of rational surfaces over arbitrary fields. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(1):19–43, 237, 1979.
- [KM14] J. Kollár and M. Mella. Quadratic families of elliptic curves and unirationality of degree 1 conic bundles. arXiv:1412.3673, 2014.
- [Kol02] J. Kollar. Unirationality of cubic hypersurfaces. *J. Inst. Math. Jussieu*, 1(3):467–476, 2002.
- [Man74] Yu. I. Manin. *Cubic forms: algebra, geometry, arithmetic*. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., New York, 1974. Translated from the Russian by M. Hazewinkel, North-Holland Mathematical Library, Vol. 4.
- [Man95] Elisabetta Manduchi. Root numbers of fibers of elliptic surfaces. *Compositio Math.*, 99(1):33–58, 1995.
- [Maz92] B. Mazur. Topology of rational points. *Experiment. Math.*, 1(1):35–45, 1992.
- [Mir89] R. Miranda. *The Basic Theory of elliptic surfaces*. ETS Editrice Pisa, 1989.
- [Riz03] Ottavio G. Rizzo. Average root numbers for a nonconstant family of elliptic curves. *Compositio Math.*, 136(1):1–23, 2003.
- [Roh93] David E. Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Math.*, 87(2):119–151, 1993.
- [Sil] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics.
- [Sil83] Joseph H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, 342:197–211, 1983.
- [Sil94] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer-Verlag, New-York, 1994.
- [STVA14] C. Salgado, D. Testa, and A. Várilly-Alvarado. On the unirationality of del Pezzo surfaces of degree two. *J. London Math. Soc.*, 90:121–139, 2014.
- [SvL14] Cecília Salgado and Ronald van Luijk. Density of rational points on del Pezzo surfaces of degree one. *Adv. Math.*, 261:154–199, 2014.
- [Tat77] J. Tate. *Number theoretic background, Automorphic forms, representations and L-functions*. Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977.
- [VA11] A. Várilly-Alvarado. Density of rational points on isotrivial rational elliptic surfaces. *Algebra & Number Theory*, 5:659–690, 2011.
- [Wil95] A. Wiles. Modular elliptic curves and Fermat’s last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.